1/2005

Datenschutz Nachrichten

28. Jahrgang
ISSN 0137-7767
9,00 Euro



Fußball-WM als Überwachungs-Großprojekt

Datenschutzverletzungen bei Internetzugängen via Satellit ■ Die Fußball-WM als Überwachungs-Großprojekt ■ Auf aussichtslosem Posten - der betriebliche Datenschutzbeauftragte? ■ Datenschutznachrichten ■ Gentechnik ■ Technik ■ Rechtsprechung ■ Buchbesprechungen ■ Pressemitteilungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Autoren dieser Ausgabe

André Adelsbach

Dipl.Inf., Horst-Görtz-Institut für IT-Sicherheit, Lehrstuhl für Netz- und Datensicherheit, Ruhr-Universität, Bochum,
andre.adelsbach@nds.rub.de, www.nds.rub.de

Ulrich Greveler

Dipl.Math., Horst-Görtz-Institut für IT-Sicherheit, Lehrstuhl für Netz- und Datensicherheit, Ruhr-Universität, Bochum,
ulrich.greveler@nds.rub.de, www.nds.rub.de

Manfred von Reumont

Datenschutzberatung und -schulung, Rheidt
info@mvr-bs.de, www.mvr-datenschutz.de

Rainer Scholl

Dipl.Kfm., Betrieblicher Datensschutzbeauftragter, Köln,
Mitglied des Vorstandes der Deutschen Vereinigung für Datenschutz
scholl@datenschutzverein.de

Dr. Thilo Weichert

Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, Kiel
weichert@datenschutzzentrum.de

Termine

17.04.2005
DVD-Vorstandssitzung in Berlin
(interessierte DVD-Mitglieder können gerne teilnehmen und melden sich bitte in der Geschäftsstelle)

15.05.2005
Redaktionsschluss DANA 2/2005
Sicherheitsbehörden und Überwachung

15.08.2005
Redaktionsschluss DANA 3/2005
Gesundheitskarte

15.11.2005
Redaktionsschluss DANA 4/2005
Big Brother Award 2005

DVD mit neuem Vorstand

Am 7. November 2004 fand in Bonn die jährliche Mitgliederversammlung der DVD statt.

Der Vorstand berichtete über die vielfältigen Aktivitäten des abgelaufenen Jahres.

Aus beruflichen Gründen legten der Vorsitzende Dr. Thilo Weichert und der stellvertretende Vorsitzende Hajo Köppen ihre Ämter nieder. Die Mitgliederversammlung dankte ihnen für ihre langjährige kompetente Tätigkeit für die DVD. Beide werden die DVD in Zukunft noch als Beisitzer im Vorstand unterstützen.

Sönke Hilbrans, Rechtsanwalt in Berlin und bisher Beisitzer im Vorstand wurde zum neuen Vorsitzenden gewählt.

Karin Schuler, Beraterin für Datenschutz und IT-Sicherheit in Bonn schied satzungsgemäß als Beisitzerin aus und wurde zur neuen stellvertretenden Vorsitzenden gewählt.

Hans-Jürgen Burger, Berater für Datenschutz und IT-Sicherheit aus Leipheim wurde erstmalig als Beisitzer in den Vorstand gewählt.

Ihre satzungsmäßige Amtszeit setzen Roland Schäfer als stellvertretender Vorsitzender, Werner Hülsmann, Rainer Scholl und Dr. Holger Taday als Beisitzer fort.

Es schloß sich eine Diskussion über die Perspektiven der weiteren DVD-Arbeit im Jahre 2005 an. Relevante Themen werden u.a. das Informationsfreiheitsgesetz, das Auditgesetz, Genomanalysen, der Lauschangriff, TKÜV und Vorratsdatenspeicherung, Videoüberwachung, die Gesundheitskarte und eventuell das von der Bundesregierung lange versprochene Arbeitnehmerdatenschutzgesetz sein.

Karin Schuler, für die DVD Mitglied in der Jury für die Big Brother Awards, berichtete anschließend ausführlich über die Auswahl der Kandidaten des Jahres 2004 sowie die Preisverleihung in Bielefeld. *(rs)*

DANA

Datenschutz Nachrichten

ISSN 0137-7767

28. Jahrgang, Heft 1

Herausgegeben

Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftsstelle:
Bonner Talweg 33-35, 53113 Bonn,
Fon 0228-222498,
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)

Rainer Scholl
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Bonner Talweg 33-35, 53113 Bonn
dana@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren

Druck

as-druck,
Nikolausstraße 43, 53129 Bonn,
Fon 0228-232425

Bezugspreis

Einzelheft 9 Euro. Jahresabonnement 32 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos.
Ältere Ausgaben der DANA können teilweise noch in der Geschäftsstelle der DVD bestellt werden.

Leserbriefe

Leserbriefe sind erwünscht, deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Anzeigen

Zur Zeit gilt Anzeigenpreisliste Nr. 1/2005

Titelbild: Rainer Scholl

Danke!

Acht Jahre lang hat Hajo Köppen als Chefredakteur für die DANA verantwortlich gezeichnet. Er hat Aufsätze und Nachrichten zusammengestellt, selber Artikel geschrieben, das Layout gestaltet und einiges an anderen organisatorischen Aufgaben dazu bewältigt. Diese Aufgabe hat er nun in meine Hände gegeben. Daher darf ich zunächst einmal Danke sagen für den unermüdlichen Einsatz, für Dutzende informative DANAs, die die anderen Leser hoffentlich genauso gerne gelesen haben wie ich.

Ich möchte die DANA auf dem gleichen hohen Niveau fortführen. Dazu bedarf es auch weiterhin der Mithilfe der Autoren, die mit ihren Beiträgen in der DANA den Datenschutz fördern wollen. Aber auch die Leser möchte ich aufrufen, ihre Wünsche zu artikulieren. Anregungen und Kritik sind jederzeit willkommen, Leserbriefe und Aufsätze neuer Autoren gerne gesehen.

Diese Ausgabe der DANA erscheint in einem neuen Layout, das den Lesern hoffentlich gefällt. Die inhaltliche Struktur bleibt unverändert: André Adelsbach und Ulrich Greveler zeigen die Gefahren von Internetzugängen via Satellit auf. Dr. Thilo Weichert formuliert Datenschutzkritik an der Ticket-Vergabe bei der kommenden Fußball-Weltmeisterschaft. Die begrenzten Möglichkeiten des betrieblichen Datenschutzbeauftragten, die betriebliche Selbstkontrolle des Datenschutzes zu gewährleisten, ist Gegenstand einer Diskussion, die von Manfred von Reumont angeregt wird. Wie gewohnt gibt es außerdem Datenschutznachrichten aus aller Welt, die neueste Rechtsprechung zu datenschutzrelevanten Themen sowie Besprechungen neuer interessanter Bücher.

Rainer Scholl

Inhalt

André Adelsbach und Ulrich Greveler*

Datenschutzverletzungen bei Internetzugängen via Satellit

1. Einführung

Viele geostationäre Satelliten sind mit digitaler Funktechnik ausgestattet und können neben Fernseh- und Rundfunkprogrammen auch Daten breitbandig übertragen. Insbesondere für strukturschwache Regionen, wo es keinen schnellen Zugang (DSL) zum Internet gibt, stellt der satellitengestützte Zugang ein interessantes Angebot für Privatanwender dar. Der PC des Teilnehmers muss dazu über eine DVB-Karte und eine Verbindung zu einer herkömmlichen Satellitenschüssel mit Digital-LNB verfügen. Dann können Internet-Verbindungen über eine Wählleitung hergestellt werden, für die ein breitbandiger Rückkanal über Satellit bereitgestellt wird. Der Durchsatz für den Rückkanal via Satellit beträgt in der Theorie bis zu 40 MB/s, ist allerdings für niedrigpreisige Angebote für Privatanwender i. a. auf Durchsatzraten, die auch im DSL-Bereich verfügbar sind, gedrosselt (z. B. 768 kB/s). Auf diese Weise kann eine Vielzahl von Usern den Dienst auf derselben Frequenz nutzen.

Der Downlink einer Satellitenverbindung (das sind die Funksignale, die der Satellit absendet) kann grundsätzlich von jeder Satelliten-Schüssel in der Ausleuchtzone empfangen werden, nicht nur vom beabsichtigten Empfänger. Dazu muss die DVB-Karte im PC lediglich auf einen Daten-Transponder eingestellt werden und in einen entsprechenden Modus versetzt werden; dann werden alle Daten-Pakete empfangen - auch wenn diese nicht für den Empfänger bestimmt sind. Software-Werkzeuge zur Gewinnung von Datenmitschnitten und deren Auswertung sind frei verfügbar im Internet zu finden. Aus technischen Gründen ist es nicht mög-lich, festzustellen, ob Daten abgehört werden, da diese von jeder Satelliten-Schüssel aufgefangen werden und es keinen Rückkanal gibt, der es dem Sender ermöglicht zu überprüfen, ob und durch wen die Daten empfangen wurden.

Aufgrund dieser Eigenschaften von Satelliten-Verbindungen spielen Sicherheitseigenschaften eine bedeutende Rolle; insbesondere Verschlüsselung ist als Schutz vor Abhören der Verbindung unumgänglich. Unsere Untersuchungen haben jedoch gezeigt, dass es eine hohe Zahl von unverschlüsselten Datenverbindungen von privaten wie kommerziellen Anwendern gibt und dass diese teilweise hoch vertrauliche Daten enthalten [NT04, AG05]. Eine bessere Aufklärung über die Risiken von Internet-via-Satellit-Anbindungen ist daher unumgänglich.

Anbieter von Internet-via-Satellit-Zugangsdiensten

Kunden in Deutschland können aus einer Vielzahl von europäischen Anbietern (Satelliten-Internet-Service-Provider, kurz Sat.-ISP) auswählen, hier eine Auswahl, die keinen Anspruch auf Vollständigkeit erhebt:

- Telekom / T-Online: »T-DSL via Satellit« (Downlink: 1024 kBit/s)
- Strato: »SkyDSL« (Downlink: bis zu 4000 kBit/s)
- Filiago: »DSL by Call« und »Sat-Flat« (Downlink: bis zu 1536 kBit/s)
- Netsystem: »ADSL via Sat« (Downlink: bis zu 300 kBit/s)

Die angebotenen Verträge sind Abonnements, Flatrates und Pay-per-Call-Zugänge, so dass den Kunden eine ähnliche Auswahl wie bei herkömmlichen Internetzugängen geboten wird. Die Preise sind im Wesentlichen abhängig von Übertragungsmenge und Durchsatzrate. Um einen Zugang nutzen zu können, muss der PC neben der Modem-/ ISDN-Verbindung eine Empfangsschnittstelle (DVB-Karte) enthalten, die via Kabel mit einer Satellitenschüssel (mit Digital-LNB) verbunden ist, dabei kann i. a. die Schüssel, die gleichzeitig zum TV-Empfang benutzt wird, Verwendung finden, so dass viele Benutzer lediglich eine DVB-Karte (ca. 100-200€) anschaffen müssen, wenn sie sich für Internet-via-Satellit entscheiden. Da die letzte Meile zum Kunden hier eine Luftschnittstelle ist, kann prinzipiell jeder europäische Anbieter ausgewählt werden, eine Beschränkung auf nationale Anbieter besteht nicht.

Wie Infratest zum Jahresende 2004 ermittelte, stieg die Zahl der deutschen Satellitenhaushalte um über eine Million auf insgesamt 15,47 Millionen (+7%) an. Via Satellit werden somit fast die Hälfte (43%) der deutschen Haushalte versorgt. Datendienste via Satellit können daher einer bedeutenden Zielgruppe angeboten werden.

2. Sicherheits- und Datenschutzproblematik

2.1. Ergebnisse von Untersuchungen zu sensitiven Daten im Broadcast-Datenstrom

Unsere Untersuchungen haben deutlich gemacht, dass eine hohe Zahl als hochvertraulich einzustufende Daten ungeschützt über den Downlink-Datenstrom abgestrahlt wird [AG05]. So konnten wir anhand eines 24h-Mitschnitts umfangreiche personenbezogene Daten (Name, Adresse, Kartennummer, Einkommen, etc.) von mehreren Personen nachweisen und die E-Mail-Korrespondenz zwischen kommerziellen Nutzern des Internet beobachten

* Horst-Görtz-Institut für IT-Sicherheit, Lehrstuhl für Netz- und Datensicherheit, Ruhr-Universität, 44780 Bochum, www.nds.rub.de

(z.B. Angebotsunterlagen militärischer Zulieferer). Dies ist umso erstaunlicher, wenn man berücksichtigt, dass die grundsätzliche Möglichkeit, Broadcast-Daten abzuhören, bereits seit Jahren in der Fachwelt bekannt ist [Dis97] und Absicherungsmöglichkeiten existieren.

Folgen des Fehlverhaltens privater Anwender

Private Internetuser, die Satellitenzugänge ungeschützt nutzen, lassen zu, dass die Daten die sie abrufen, in der Ausleuchtzone des Satelliten (Mitteleuropa im Falle von Astra 1E) ausgestrahlt werden. Dies betrifft sowohl private Kommunikation (E-Mail) als auch die Inhalte die bei Nutzung des WWW ausgetauscht werden. Da jeder Nutzer eines ungeschützten Zuganges eine eindeutige Hardwarekennung (die MAC-Adresse der DVB-Karte) besitzt, die in jedem ausgestrahlten Datenpaket enthalten ist, können durch den Abhörenden auf einfache Weise Profile erstellt werden, so dass einem Nutzer beispielsweise die abgerufenen Webseiten, die eingegebenen Suchbegriffe bei Suchmaschinen, empfangene Chat-Nachrichten, Transaktionen bei Online-Plattformen, heruntergeladene Dateien (aus möglicherweise illegalen Quellen), Namen und E-Mail-Adressen seiner Kommunikationspartner etc. automatisiert zugeordnet werden können. Auf diese Weise lassen sich umfangreiche Dossiers über Personen erstellen (siehe Abb. 1)

Zu dieser Vertraulichkeitsproblematik kommt noch der Sicherheitsaspekt hinzu. Durch geschicktes Nutzen von Informationen aus automatisch versandten E-Mails und Browser-Cookies (das sind Steuer-Informationen beim Abrufen von Webseiten) kann ein Angreifer User-Identitäten stehlen, indem er Protokolle zur Änderung von Passwörtern ausführt. Die dazu benötigten Informationen können, wie unsere Untersuchungen ergaben, vollständig dem abgehörten Datenstrom entnommen werden. Der Angreifer kann dann ein User-Konto (z. B. für ein Online-Auktionshaus) weiternutzen und in fremden Namen Transaktionen ausführen, während der legitime Besitzer der Identität ausgesperrt wird.

Folgen des Fehlverhaltens kommerzieller Anwender

Kommerzielle Internetnutzer, die Satellitenzugänge verwenden, haben ein besonderes Augenmerk auf die Absicherung der Verbindung zu legen, insbesondere wenn sensitive Daten ihrer Kunden übertragen werden. Bei der Untersuchung wurde jedoch festgestellt, dass nicht alle kommerziellen Nutzer dieser Verpflichtung nachkommen. Besonders erschreckend war die Tatsache, dass Onlineshops identifiziert wurden, die ihren Kunden einen sicheren Zugang über das Internet anboten (hier: SSL-Verschlüsselung), aber die vom Kunden übermittelten sensitiven Daten dann über unsichere Kanäle (ungeschützte Satellitenverbindung eines Satelliten-ISP) vom Webserver an die interne Buchhaltung weiterleiteten. Wenn solche Daten abgehört werden, liegen die von den Kunden übermittelten personenbezogenen Daten in strukturierter Form vor und können von Unbefugten ohne technischen Aufwand weiterverarbeitet werden.
Neben sensiblen Kundendaten wurden auf diese Weise zahlreiche interne Firmen-Emails ungeschützt über Satelliten-Internetverbindungen abgerufen (siehe Abb. 2). Unsere Untersuchungen zeigten, dass auf diese Weise Angebotskalkulationen, geheime Produktinformationen und Bewerbungsunterlagen abgerufen und unwissentlich über Mitteleuropa verbreitet werden. Der potentielle wirtschaftliche Schaden lässt sich nur schwer quantifizieren, dürfte jedoch in Einzelfällen mehrere Millionen Euro betragen.

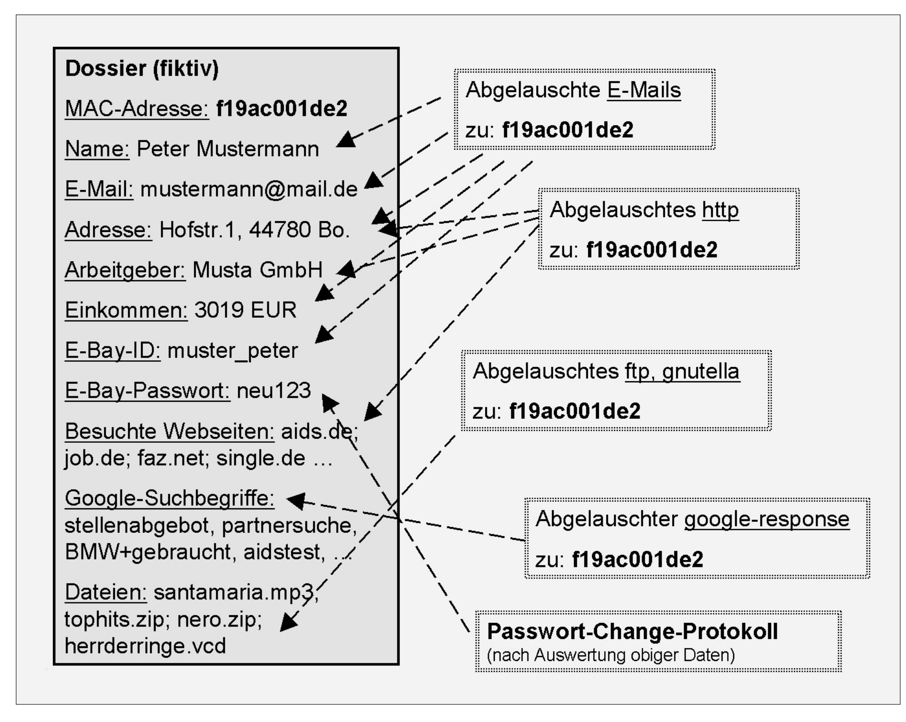


Abb. 1: Zuordnung personenbezogener Daten zu einer Person anhand der MAC-Adresse

2.2. Wie können Verbindungen abgesichert werden?

Prinzipiell existieren mehrere Alternativen zur Absicherung von Satelliten-Internetzugängen. Im Folgenden betrachten wir die möglichen Alternativen und diskutieren deren Vor- und Nachteile.

Absicherung durch dedizierte Proxy-Software

Eine Satelliten-Anbindung hat aufgrund der geostationären Position des Satelliten eine hohe Signal-Laufzeit (ca. 0,5 s), die eine hohe Latenz bedingt und im Extremfall sogar Un-terbrechungen bei Datenverbindungen provozieren kann. Um diese Gesamtlatenz zu verringern bzw. deren Auswirkung auf die Verbindung zu minimieren, bieten viele Satelliten-ISPs eine spezielle Software (engl. Performance Enhancing Proxy) an, die neben durchsatzsteigernden Maßnahmen (beispielsweise Pre-Fetching von Bildern einer angefragten Webseite oder TCP-Pre-Acknowledgements, beides technische Maßnahmen zur Beschleunigung der Datenverbindung) auch zur Verschlüsselung des Downlinks verwendet werden kann.

Um die Proxy-Software (und somit

deren Sicherheitsfunktionen) zu nutzen, müssen Benutzer ihre Anwendungen (z.B. Web-Browser und Mailanwendung) so konfigurieren, dass diese über die lokale Proxy-Software kommunizieren. Dadurch wird auch eine Absicherung der Daten implizit erzwungen. Die Antworten vom Satelliten-Proxy werden erst vom PC selbst entschlüsselt und an die Anwendung bzw. den Nutzer weitergereicht.

Der Vorteil dieser Lösung ist, dass sich Sicherheit und Durchsatzsteigerung gleichzeitig mit einer Software erzielen lassen, die der Nutzer vom Anbieter erhält und ohne technisches Wissen einfach »aktivieren« kann. Auf der anderen Seite hat diese Lösung auch einige Nachteile. Zum einen wird keine Ende-zu-Ende-Sicherheit erreicht, da die Daten nur zwischen Satellit und Endbenutzer verschlüsselt übertragen werden, d. h. in Netzknoten beim Anbieter laufen zunächst alle Daten unverschlüsselt an. Des Weiteren gibt es Konflikte mit etablierten Sicherheitstechnologien wie beispielsweise IPSec, das auf der Netzwerkschicht arbeitet, da der Satelliten-Proxy in das TCP-Protokoll eingreift. Ein weiterer wesentlicher Nachteil besteht darin, dass die Proxy-Software meist proprietäre Sicherheitsmechanismen verwendet und nicht öffentlich spezifiziert ist. Dies verhindert eine Sicherheitsanalyse durch unabhängige Experten, die wesentlich zur Sicherheit offener Sicherheitsstandards wie IPSec oder TLS beigetragen haben. Trotz dieser Nachteile ist diese grundsätzliche Absicherung der Verbindung mittels Proxy-Software immer einer unverschlüsselten Übertragung vorzuziehen, wenn sensitive Daten übertragen werden.

From: ----------- R LtCol -- SFS/-- [mailto:------@------.af.mil]
Sent: Friday, November 12, 2004 4:06 AM
To: ----------; ------------- F TSgt -- SFS/SF---
Cc: ----------; ----------; ----------; ---------- LtCol
-- SFS/--; ---------- Capt 31 SFS/---; ---------- SMSgt 31 SFS/---
Subject: RE: ---------- System

Mr. ----------,
We would greatly appreciate a sooner installation. We have troops that need this training and can no longer afford to have our system sitting in a warehouse. Let me know if there is anything I can do to help.
Thank you. Lt Col ----------

-----Original Message-----
From: ---------- [mailto:----------.co.uk]
Sent: Friday, November 12, 2004 10:02 AM
To: ---------- TSgt 31 SFS/SF---'
Cc: LtCol 31 SFS/CC'; ------ Capt 31 SFS/---'; ------ SMSgt 31 SFS/---'
Subject: RE: ---------- System

TSgt ----------,
I will contact the Installation and Training team at headquarters in Atlanta USA to see if they can get your system installed sooner.
Regards ----------

(...)
From: ---------- F TSgt 31 SFS/SF---
[mailto:----------@----------.af.mil]
Sent: 12 November 2004 08:43
To: ---------- Cc: ----------; ----------; ----------; ---------- LtCol
31 SFS/--; ---------- Capt 31 SFS/SFT; ---------- SMSgt 31 SFS/---
Subject: RE: ---------- System

All: We would really like to have the -------- set up before then, if you have the resources, please check and see what you can do for our unit. If you can't do it then we would like it done on the first available date that you have. I will be awaiting your response. Thanks for your help in advance.
TSgt ---------- ---------- Training

Abb. 2: abgehörte E-Mail-Konversation von Militärzulieferer (»-----« wurde zur Anonymisierung verwendet)

Ende-zu-Ende-Absicherung durch VPN

Eine VPN-Lösung (z. B. Ende-zu-Ende-Verschlüsselung und Einbindung des Clients in ein LAN via VPN-Router) kann für einige der Satelliten-Zugänge grundsätzlich eingerichtet werden; leider gibt es dabei jedoch erhebliche Performance-Einbußen, da einige Sat.-Proxy-Technologien (z. B. Pre-Acknowledgements) nicht verwendet werden können. Des Weiteren eignet sich diese Technologie primär dazu, die Kommunikation zwischen Rechnern mit Vertrauensbeziehungen, z.B. die Rechner einer logischen Einheit (Unternehmen), zu sichern und zu einem virtuellen lokalen Netzwerk zu verbinden, nicht jedoch, um sicher mit beliebigen Web-Servern zu kommunizieren.

Die VPN-Lösung ist daher nur in Spezialfällen anwendbar, beispielsweise um einen Heimarbeitsplatz sicher über SAT-ISPs in ein Firmennetz einzubinden. Die Kommunikation mit Rechnern außerhalb des Firmennetzes (z.B. Web-Server einer Bank oder eines Online-Auktionshauses) muss durch alternative Maßnahmen gesichert oder unterbunden werden.

Absicherung einzelner Dienste durch den Nutzer

Wenn sich der User auf einzelne Dienste beschränkt und keine weiteren Dienste über den Broadcast-Kanal genutzt werden, können diese dediziert (auch von Dritten) auf Anwendungsebene abgesichert werden.

Sicherheitsmaßnahmen auf Anwendungsebene (beispielsweise SSL/TLS beim »Surfen« im Internet) eignen sich aber auch (alternativ oder komplementär zu VPN-Lösungen) dazu, um Home-Office-Mitarbeitern sicheren Zugang zu Diensten des Firmennetzwerkes zu bieten. In diesem Kontext sind SMTP / POP3 zum Versenden / Abholen der E-Mail und HTTP zum Zugriff auf das Intranet des Arbeitgebers als häufigste Dienste zu nennen, auf die die Kommunikation beschränkt werden könnte.

Gleichzeitig kann jeder Arbeitgeber bei Homeoffice-Arbeitsplätzen Vorsorge treffen, indem er keine unverschlüsselten Zugänge (zum E-Mail-Server oder Intranet) anbietet. So stellt er sicher, dass keine sensiblen Daten über unsichere Kanäle (z.B. ungeschützte Satellitenverbindungen oder WLANs mit schwacher Verschlüsselung) abgerufen werden können, da diese immer ver-

schlüsselt zum Anwender transportiert werden und daher keine Abhängigkeit von sicheren Übertragungswegen gegeben ist.

3. Fazit

Die von uns durchgeführten Untersuchungen haben gezeigt, dass trotz existierender Sicherheitsmaßnahmen personenbezogene und vertrauliche firmeninterne Daten ungeschützt via Satellit ausgestrahlt werden, da Internet-via-Satellit-Zugänge ohne Absicherung der Daten genutzt werden. Die Ursachen dafür sind entweder in der Unkenntnis privater wie kommerzieller Nutzer oder in fahrlässiger Verhaltensweise zu suchen; ungewollte Auswirkungen sind umfangreiche Verletzungen von Persönlichkeits- wie Datenschutzrechten und potentieller wirtschaftlicher Schaden.

Wir sehen die Anbieter der Netzzugänge hier in der Pflicht, ihre Kunden über diese Gefahren aufzuklären. Wir haben gezeigt, dass es technisch möglich ist, festzustellen, welche Nutzer aufgrund fehlerhafter Konfiguration oder leichtsinnigen Verhaltens zu dieser Problematik beitragen und inwieweit personenbezogene Daten übertragen werden; die Anbieter könnten ihrerseits diese Nutzer unter ihren Kunden automatisiert aufspüren und gezielt informieren, da ihnen die Zuordnung von Hardware-Adresse und Kundenkennung schon aufgrund der Vertragsdaten zugänglich ist. Wenn die betroffenen Kunden gezielt über die Folgen ihres Tuns informiert würden, wäre eine Verbesserung der Situation zu erwarten. Insbesondere kommerzielle Nutzer, die Daten ihrer Kunden unwissentlich nicht schützen, haben eine hohe Motivation, diesen Missstand zu beheben, da sie Haftungsansprüche fürchten müssen, wenn sie nach der Aufklärung weiterhin sensitive personenbezogene Daten ungeschützt ausstrahlen.

Literatur

[AG05] André Adelsbach und Ulrich Greveler. Satellite Communication without Privacy (Sicherheit 2005, 2. Jahrestagung, Fachbereich Sicherheit d. Gesellschaft für Informatik). Bericht, April 2005.

[Dis97] Dr Dish. Digital data from the sky. Zeitschriftenartikel 10/97, TELE-satellite International Magazine, Oktober 1997.

[DB04] Heise News-Ticker (Daniel Bachfeld). Forscher spähen Satelliten-Internet-Zugänge aus. Tickermeldung, http://www.heise.de/newsticker/meldung/53676, November 2004.

Dr. Thilo Weichert

Die Fußball-WM als Überwachungs-Großprojekt

»Die Weltmeisterschaft wird von Sponsoren und Überwachungsindustrie missbraucht, um Schnüffeltechnik einzuführen und die Fans auszuspionieren«. Diese Vermutung von Rena Tangens vom FoeBuD e.V. in Bielefeld wird vom Bündnis Aktiver Fußball-Fans (BAFF) geteilt. Deren Sprecher Jörg Höfer meint: »Wenn Fußballfans nur die Wahl haben, teilweise sehr persönliche Daten preiszugeben, ohne zu wissen, wer darauf Zugriff hat, oder eben keine Tickets zu bekommen, wird die Verhältnismäßigkeit der Mittel nicht gewahrt und das Grundrecht auf informationelle Selbstbestimmung verletzt«. Und aktuell wird wieder der frühere Leiter des ULD, Helmut Bäumler, in der Presse zitiert, der schon vor einigen Monaten in einem ARD-Interview meinte, an der Fußball-WM entlarve sich, dass die RFID-Technik nur ein Ziel habe: Das Tracking von Menschen, also das Verfolgen und Erstellen von Bewegungsprofilen.[1]

Im Folgenden wird näher untersucht, ob diese kritischen Stimmen zum Ticketverkauf für die Fußballweltmeisterschaft 2006 zutreffen.

I. Das Konzept

Vom 01.02.2005 an konnten Tickets für die Fußball-Weltmeisterschaft in Deutschland im Jahr 2006 bestellt werden. Damit begann die erste von vier Verkaufsphasen, deren letzte am 15.04. 2006 beendet sein soll. Kurz vor dem Bestellbeginn veröffentlichte das Organisationskomitee Deutschland FIFA Fußball-Weltmeisterschaft Deutschland 2006 (OK) die Allgemeinen Vertragsbedingungen sowie die gesamte Verkaufs- und Kontrollstrategie. Diese ist von zwei Zielsetzungen beseelt: Die größtmögliche Sicherheit soll in den Stadien gewährleistet werden. Außerdem soll der Schwarzhandel mit den Tickets ausgeschlossen werden. Um diese Ziele zu erreichen, setzt das Organisationskomitee, das rechtlich Teil des Deutschen Fußballbundes[2] ist, auf die Personalisierung der Tickets: Bei der Bestellung der Tickets müssen die Interessentinnen und Interessenten Identifizierungsdaten angeben. Die Tickets erhalten einen RFID-Chip, über den eine eindeutige Zuordnung zu der durch das Ticket berechtigten Person hergestellt werden kann, da sämtliche Berechtigte in einer DFB-Datenbank gespeichert werden. Die Ticket-Kontrolle erfolgt per RFID-Leser an den Eingangsschleusen der Stadien. Möglich sind auch im Vorfeld von Spielen außerhalb der Stadien Kontrollen, bei de-

[1] zit. nach www.foebud.org

[2] DFB, Otto-Fleck-Schneise 6, 60526 Frankfurt am Main

nen die in der DFB-Datenbank gespeicherten Angaben mit denen auf möglichst mitzuführenden Personalausweisen oder Reisepässen abgeglichen werden sollen.

Schon das Grundkonzept muss aus Datenschutzsicht hinterfragt werden. Es ist nicht nachvollziehbar, weshalb eine vollständige Personalisierung sämtlicher Stadionbesucher erfolgen muss. Die Zielsetzung, Schwarzhandel zu verhindern, erscheint insofern nur vorgeschoben. Hierfür wäre die umfassende Personalisierung auch unverhältnismäßig. Tatsächlich scheinen zwei Gründe im Vordergrund zu stehen:

Zum einen ist die Personalisierung der RFID-Tickets ein Großprojekt zur Förderung dieser Technologie im Konsumentenbereich. So sinnvoll die RFID-Technologie in vielen Wirtschaftssektoren sein mag, z.B. bei der Logistik, so gefährlich ist sie bei der Personalisierung, insbesondere wenn dadurch im weitesten Sinn allgemein Verbraucherinnen und Verbraucher betroffen sind. Die Personalisierung verfolgt unzweifelhaft das Ziel der Manipulation und der Kontrolle der Verbraucherverhaltens, zielt also letztendlich statt des selbstbestimmten anonymen Konsums auf den fremdbestimmten Konsum. Die RFID-Technologie, eingesetzt in Produkten, auf Kundenkarten oder eben auf personalisierten Tickets, ist wie keine andere geeignet, diese Konsumentenkontrolle zu verwirklichen.

Mit der Personalisierung der Tickets soll der »gläserne Fußballfan« mit dem Ziel erhöhter Sicherheit in den Stadien Realität werden. Stadienverbote sollen dadurch effektiv umgesetzt werden; durch die Möglichkeit des Abgleichs mit Gewalttäter- und Hooligan-Dateien meint man, mehr Sicherheit zu schaffen. Überwachung ist nicht mit Sicherheit gleichzusetzen. Diese Vorstellung wäre eine gefährliche Illusion. Im Vorfeld des Stadionbesuchs besteht keine Vorlagepflicht des Tickets. Kontrollen können hier problemlos allein über Ausweiskontrollen realisiert werden. Wegen des Massenandrangs an den Nadelöhren der Ticketprüfung an den Stadioneingängen können dort keine Personenkontrollen durchgeführt werden. Allenfalls Stichprobenkontrollen sind möglich. Dies bedeutet: Hooligans können sich problemlos Tickets dadurch beschaffen, dass sie sich durch nicht vorbelastete Personen bestellte Karten weitergeben lassen, ohne dass ein großes Entdeckungsrisiko besteht. Statt der trügerischen Sicherheit durch Totalpersonalisierung sollten von Veranstaltern und Polizei die klassischen Sicherheitsmaßnahmen ergriffen werden: Erkennbare Präsenz von Sicherheitspersonal, das deeskalierend interveniert.

Ergebnis ist, dass schon das Gesamtkonzept der Ticketvergabe mit dem Datenschutz nicht vereinbar ist. Verletzt wird insbesondere der Grundsatz der Datenvermeidung und Datensparsamkeit (§ 3a BDSG). Dieser verlangt, dass bei unterschiedlichen Konzeptalternativen jeweils die gewählt werden muss, bei der am wenigsten personenbezogene Daten erhoben werden und dadurch die geringstmögliche Überwachung der Menschen stattfindet.

II. Der Bestellvorgang

Die Bestellung der Tickets wird über Formulare ermöglicht, die verschickt werden und im Internet verfügbar sind und ausgefüllt per Post verschickt werden können. Möglich ist auch die Online-Bestellung über Internet oder die Bestellung per Fax. Die Zusendung der Bestätigung der Berücksichtigung bei der Kartenverteilung erfolgt entweder per Email oder per Post. Über Internet wird auch die Möglichkeit eröffnet, jederzeit den Status der eigenen Bestellung festzustellen und zu verfolgen. Die Bezahlung soll in jedem Fall bargeldlos erfolgen, wobei es drei Alternativen gibt. Erste Priorität hat das Bezahlen mit einer bestimmten Kreditkarte, der MasterCard. Ist eine solche nicht vorhanden, so können Bestellungen in Deutschland nur über ein Banken-Lastschriftverfahren vorgenommen werden. Lediglich für Bestellungen aus dem Ausland wird auch die Bezahlung per Überweisung akzeptiert.

Aus Datenschutzsicht ist das Bestellformular zu kritisieren: Selbst wenn eine personalisierte Bestellung akzeptiert würde, so wird ein Übermaß an Daten erhoben. Es ist überhaupt nicht erkennbar, weshalb das genaue Geburtsdatum angegeben werden muss. Dieses Datum ist für die Werbebranche von großem Wert, weil hierüber Datenbanken miteinander verknüpft werden können. Für die Kartenbestellung ist es überflüssig. Hier würde die Feststellung der vollen Geschäftsfähigkeit, also die Angabe »älter als 18 Jahre« ausreichen.

Ebenso nicht erforderlich erscheint die Angabe der Personalausweis- oder Passnummer mit genauen Angaben zur Nationalität, zur ausstellenden Behörde und zum Ausstellungsdatum. Das Organisationskomitee erklärte, dass es diese Nummer nicht als Ordnungsmerkmal nutzen werde. Deren Verwendung zum Erschließen von Dateien wäre unzulässig (§§ 3 Abs. 4, 4 Abs. 2 PAuswG). Die Polizei dürfte zwar die Ausweisnummer überprüfen. Dieser gegenüber besteht aber außerhalb des Stadions keine Pflicht zur Vorlage des Tickets. Auch für Zwecke der Polizei macht die Nummer keinen rechten Sinn. Bisher ist nicht bekannt, dass geplant ist, dass die Daten (sämtlicher?) Ticketbewerber präventiv an die Polizei übermittelt werden, um an Hand dieser Datenbestände Hooligans herausfiltern. Ein solches Vorgehen wäre auch unzulässig: Da die dateimäßige Erfassung der Ausweisnummer zunächst durch das Organisationskomitee erfolgt, wäre schon ein Verstoß gegen § 4 Abs. 2 PAuswG gegeben, da der Zweck der Speicherung die Verknüpfung mit Polizeidateien ist. Aber auch diese Verknüpfung wäre unzulässig, da die Daten auf Grund eines Vertrages bzw. per Einwilligung erhoben werden. Nicht einmal im Kleingedruckten der Vertragsformulare ist aber ein Passus zu entnehmen, dass (sämtliche ?) Ticket-Bewerber polizeilich gegengecheckt würden bzw. werden dürften. Die in den Datenschutzbestimmungen enthaltene Formulierung (»Der DFB (OK) ist berechtigt, diese Daten an Sicherheitsbehörden zu übermitteln, soweit dies im Einklang mit den gesetzlichen Vorschriften erforderlich ist«) gibt für einen Abgleich nichts her. Eine anlasslose Übermittlung an die Polizei ist eben weder erforderlich noch gesetzlich vorgesehen. Eine solche Rasterfahndungsmaßnahme wäre von Polizeiseite nach dem jeweiligen Polizeirecht zu beurteilen. Danach (z.B. in Schleswig-Holstein § 195 LVwG SH), wäre der Datenabgleich i.d.R. nicht zu rechtfertigen. Hinzu kommt, dass in den einschlägigen Polizeidateien, z.B. über Hooligans, die Personalausweisnummer überhaupt nicht vermerkt sind.

Korrekt ist auf dem Formular der Hinweis, dass die Angabe von Telefonnummer, Faxnummer und Email-Adresse freiwillig ist. Weshalb diese Daten (außer Email-Adresse) nötig oder zumindest sinnvoll sein könnten, ist aber nicht erkennbar. Die für die Online-Kommunikation genutzte Email-Adresse bietet eventuell einen Komfortvorteil. Deren Nutzung zwecks Unterrichtung von Nachrückern bei der Vergabe

Innenministerium und DFB verteidigen WM-Datenerhebung

Das von Datenschützern heftig kritisierte Bestellverfahren für Fußball-Weltmeisterschafts-Tickets haben die deutschen Sicherheitsbehörden maßgeblich mitgestaltet. Das Bundesinnenministerium (BMI) bestätigte, dass selbst die Details der Datenerhebung des Ticketverfahrens zwischen dem WM-Organisationskommitee (OK) des Deutschen Fußballbundes (DFB) und deutschen Sicherheitsbehörden abgestimmt worden sind. BMI-Sprecherin Gaby Kautz meinte, mit Blick auf die Sicherheitsinteressen Deutschlands zur WM 2006 sei die Erhebung der Reisepass- oder Ausweisnummern erforderlich. Auch das Geburtsdatum müsse abgefragt werden. Der Datenumfang beruhe auf einer Empfehlung des Ständigen Ausschusses zur Gewaltkonvention des Europarates sowie Erfahrungen der Ausrichter vergangener Welt- und Europameisterschaften.

Um Hooligans am Besuch der Spiele zu hindern, sollen die Daten der Ticketbewerber mit der beim DFB geführten Hausverbotsdatei/Stadionverbotsdatei abgeglichen werden. Dieser Abgleich geschehe beim DFB und nicht bei der Polizei. Kautz: »Ein solcher Abgleich ist auch bei der Zuteilung von Tickets für Länderspiele europaweit gängige Praxis«. Es sei nicht geplant, dass die vom DFB gesammelten persönlichen Daten der Kartenbesteller vorsorglich den Sicherheitsbehörden übergeben werden. Dass die Besucherdaten dennoch in Polizeicomputern landen, wollte Kautz nicht ausschließen. Sollte eine Straftat zu verhindern oder eine Gefahr für die öffentliche Sicherheit oder Ordnung abzuwehren sein, könnten die vom DFB erhobenen Personendaten der Polizei übermittelt werden. Dies erlaube das Bundesdatenschutzgesetz (§ 28 Abs. 3 Nr. 2). Darüber hinaus seien weitere Erhebungsbefugnisse gültig, z.B. § 163 Strafprozessordnung und die Gefahrenabwehrvorschriften der Landespolizeigesetze.

Ob diese Angaben zutreffen, kann bezweifelt werden, zumal Bundesinnenminister Otto Schily (SPD), der auch im Aufsichtsrat des OK sitzt, auf der 4. Sicherheitskonferenz zur WM 2006 im November 2004 in Berlin erklärte: »Wir schaffen damit eine nationale Stelle, bei der alle Informationen und Analysen der zuständigen nationalen und internationalen Sicherheitsbehörden zusammenlaufen und koordiniert werden. Aus den Informationen entstehen nationale Lagebilder, die allen Beteiligten zur Verfügung gestellt werden«.

Kritik an dem Ticket-Vergabeverfahren äußerte auch der Verbraucherzentrale Bundesverband (vzbv) undhat dem DFB eine Abmahnungserklärung zugesandt. Die Allgemeinen Geschäftsbedingungen verstießen gegen das Bürgerliche Gesetzbuch. So sei es unzulässig, von den Ticketinhabern zu verlangen, bei Film- und Fotoaufnahmen im Stadion der Verwendung ihres Bildes und ihrer Stimme »unwiderruflich« und »für alle gegenwärtige und zukänftigen Medien« zuzustimmen. Der DFB verweigerte jedoch das Unterschreiben der geforderten Unterlassungserklärung: »Wir nehmen die Abmahnung nicht hin und werden auch die Unterlassungserklärung nicht unterschreiben«. Die DFB-Juristen hätten die Abmahnung geprüft und festgestellt, dass sie rechtlich nicht haltbar sei. »Vor allem gehen wir davon aus, dass es überhaupt nicht im Sinne der Fans wäre, wenn wir auf die Unterlassungserklärung eingingen.« Der vzbv betreibe »Wortklauberei«. Der vzbv kündigte an, eine Klage gegen den DFB zu prüfen (vgl. S. 11).

Der RFID-Einsatz wird von den Fußballfunktionären verteidigt. In der Arena auf Schalke 04 wird seit ihrer Eröffnung die Technik eingesetzt. Pressesprecher Gerd Voss ist begeistert: »Die Chips sind praktisch fälschungssicher; wir merken sogar, wenn jemand mit einer durch den Zaun gesteckten Karte das Stadion betreten will«. Dann leuchte in der Nähe eines Drehkreuzes eine rote Lampe auf; ein Ordner könne dann die Karte persönlich überprüfen. Um die Vorgaben des OK erfüllen zu können, müssten nur noch kleinere Änderungen vorgenommen werden, »je nachdem, welche Daten noch zusätzlich auf den Chip kommen«. Denn hinter jeder einzigartigen Nummer einer Karte hänge eine Datenbank. Das spare Geld beim Ordnungspersonal und bei der Vergabe von Dauerkarten. Der Fußballclub müsse nicht jedes Jahr neue Karten zuschicken. Die Lesegeräte wüssten, wer die Dauerkarte bezahlt habe und wer nicht.
(www.spiegel.de 03.02.2005; Lembke FAZ 02.02.2005; Kok taz NRW 22.01.2005, 2)

---

von Ticketrückläufen[3] entspräche dem vertraglichen Zweck und ist datenschutzrechtlich unproblematisch. Doch für Telefon- und Faxnummerangaben besteht zudem eine eher gefährliche Nutzungsoption: deren Verwendung für Werbezwecke, nachdem die Daten an interessierte Firmen weitergegeben wurden. Den Ticket-Bestellern ist im Zweifel zu raten, hier keine Angaben zu machen.

Als Pflichtfeld vorgesehen ist die Angabe, für welche Nationalmannschaft man »Fan« ist. Auch diese Angabe ist im Grunde nicht nötig. Zweck der Angabe ist offensichtlich, Tickets bestimmten Fan-Blocks zuzuordnen. Dies kann, auch aus Sicherheitsgründen, sinnvoll sein. Wer nicht möchte, dass seine Sympathien für eine bestimmte Mannschaft bekannt werden, der kann und der sollte das Kästchen »neutral« ankreuzen.

Folgt man der Logik, dass sämtliche WM-Besucher eindeutig identifiziert sein müssen, so ist es logisch, dass nicht nur der Besteller seine Personalien angeben muss, sondern dass auch diese Daten von weiteren Besuchern erhoben werden. Konsequent ist weiterhin, dass im Formular folgende Erklärung abverlangt wird: »Sofern meine Ticketbestellung auch Tickets für Dritte beinhaltet, erkläre ich, dass mich diese Personen ausdrücklich ermächtigt haben, die vorgenannten Bedingungen und Richtlinien auch in deren Namen anzuerkennen und diesen Personen vollständig zur Kenntnis zu bringen werden«. Papier ist geduldig. Da ohne diese Erklärung keine Tickets für Dritte bestellt werden können, werden alle diese unterschreiben. Ebenso sicher ist, dass diese Erklärung von den meisten Bestellern nicht beachtet werden wird. Da dies der DFB weiß bzw. wissen muss, muss er sich Mängel bei der Einbeziehung der Dritten zurechnen lassen. Dies gilt in jedem Fall für die Werbenutzung der Drittdaten (dazu näher unten).

Nicht mit den Regelungen zur Datensparsamkeit (§ 3a BDSG) vereinbar ist die vorgesehene elektronische Zah-

[3] vgl. FAQ Nr. 15 u. 33, www.fifaworldcup.yahoo.com/o6/de/tickets/faq.html

lungsart. Deren Konsequenz ist, dass in jedem Fall sensible Bankdaten offenbart werden müssen. Inwieweit der vorrangige und ausschließliche Einsatz einer Kreditkarte (MasterCard) rechtlich zulässig ist, ist weniger eine datenschutz- als eine wettbewerbsrechtliche Frage. Der Umstand, dass keine anonyme Art der Bezahlung (Bargeld oder Prepaid-Geldkarte) zugelassen wird, ist ein eindeutiger Verstoß gegen den Grundsatz der Datensparsamkeit. Gerade bei einem Monopol-Marktangebot, wie es der DFB-Ticket-Verkauf darstellt, müssen anonyme Zahlalternativen angeboten werden. Zusätzlich nicht einsehbar ist, weshalb das die Selbstbestimmung der Betroffenen stärker einschränkende Lastschriftverfahren gegenüber dem datensparsameren Überweisungsverfahren vollständig vorgezogen wird. Den Betroffenen wird die Wahlfreiheit zwischen Lastschrift oder Überweisung genommen. Die vorgesehene Hierarchie der Zahlungsarten mag für den DFB am praktischsten sein, für den Betroffenen bedeutet dies, dass er solche Verfahren nutzen muss, bei denen am wenigsten seine informationelle Selbstbestimmung beachtet werden.

Die Einwilligungserklärung zur Nutzung der Daten für Werbezwecke dürfte aus mehreren Gründen unwirksam sein, mit der Folge, dass eine Werbenutzung der Daten aus Datenschutzsicht zu beanstanden wäre. Zwar hat der DFB richtig erkannt, dass überhaupt eine Einwilligung erforderlich ist und dass eine Widerspruchslösung nicht ausreichend gewesen wäre. Doch leidet die genutzte Einwilligungserklärung an rechtlichen Mängeln.

Der erste Mangel besteht darin, dass keine Wahlmöglichkeit besteht zwischen reinen DFB-Informationen und der Übermittlung der Daten »für Werbezwecke an Offizielle Partner/Nationale Förderer und an die FIFA«.

Der zweite Mangel besteht darin, dass an dieser Stelle nicht erkennbar ist, wer die Sponsoren sind und man hierfür auf die Homepage der FIFAworldcup.com verwiesen wird. Da viele Fußballfans kein Internet haben dürften, sind diese von einer eigenen Informationsmöglichkeit völlig abgeschnitten. Ebenso unklar ist für den normalen Fußballfan, wer sich genau hinter der »FIFA« verbirgt. Problematisch ist weiterhin, dass keine abschließende Datenübermittlung zugesichert wird. Es ist nicht ausgeschlossen, dass die Empfänger die Werbedaten an weitere Dritte weitergeben. Der Verweis auf die »anwendbaren Datenschutzbestimmungen« hat keinerlei Aussagekraft geschweige denn eine eingrenzende Wirkung.

Der dritte und wesentlichste Mangel der Einwilligungserklärung besteht darin, dass direkt unter dem Kästchen, das man ankreuzen soll, wenn man »mit der werblichen Nutzung der Daten einverstanden« ist, folgender Text vor der abschließenden Unterschrift des Bestellers abgedruckt ist: »Zustimmung und Unterschrift - Bitte beachten Sie dass für eine Bestellung die Zustimmung zur Speicherung der persönlichen Daten und zu den ATGBs/Verkaufsrichtlinien unbedingt notwendig ist». Dieser Text ist insofern falsch, als für die zur Abwicklung des Ticket-Vertrages eine separate Zustimmung überhaupt nicht erforderlich ist. Der Vertragsabschluss legitimiert eigenständig die hierfür nötige Datenverarbeitung (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG). Diese falsche Darstellung wäre unschädlich, wenn sie nicht direkt über dem Feld zur Einwilligung in die Werbenutzung stehen würde. Selbst ein kritischer Ticketbesteller kann durch diese Formulierung nur den - falschen - Eindruck haben, »unbedingte« Voraussetzung für die Ticketbestellung wäre das Ankreuzen der Einwilligung für die Werbenutzung. Jedenfalls entstehen durch die Formulierung Zweifel. Um nicht Gefahr zu laufen, bei der Ticketvergabe unberücksichtigt zu bleiben, werden selbst Menschen, die keine Werbung haben wollen, hier ein Kreuz setzen. Dem Besteller hätte zumindest unmissverständlich mitgeteilt werden müssen, dass der Ausschluss von Werbung keinerlei Nachteile bei der Ticketbestellung zur Folge hat.

Der vierte Mangel der Einwilligung in die Werbung besteht darin, dass die Einbeziehung Dritter in die Werbenutzung ungenügend ist. Zwar bezieht sich das Einverständnis auf die Datenangaben der Dritten. Eine Wahlmöglichkeit ist aber insofern nicht vorgesehen. Diese wäre aber dringend nötig gewesen, da davon auszugehen ist, dass nicht alle von einer Bestellung zugleich erfassten Personen einen einheitlichen Willen bzgl. der Werbezusendung haben. Hinzu kommt, dass der Besteller bei einem Ankreuzen zur Werbenutzung allenfalls seine eigenen Daten im Blick hat. Ihm wird nicht bewusst sein, dass er insofern auch eine Einwilligungserklärung für Dritte abgibt. Hieran ändert auch die Erklärung nichts, dass diese Personen ihn »ausdrücklich ermächtigt haben«. Dies kann sich nur auf die Ticketbestellung, nicht aber auf die Einwilligung zur Werbenutzung beziehen. Konsequenz des vierten Mangels ist, dass in keinem Fall die Daten der Besucher für Werbezwecke genutzt werden dürfen.

III. Die weitere Datenverarbeitung

Als Datenverarbeiter im Auftrag des DFB (OK) wird - soweit aus der Presse bekannt - die Firma CTS EVENTIM AG tätig. Diese hat eigene Allgemeine Geschäftsbedingungen, die teilweise weiter gefasst sind als die des DFB (OK) (abrufbar unter www.eventim.de). In den AGB zum Datenschutz VII.2. wird die Nutzung von Kundendaten für Werbezwecke generell erlaubt, »solange der Kunde nicht widerspricht«. Weiter heißt es dort: »Diese Einwilligung kann von Ihnen jederzeit ohne Angaben von Gründen widerrufen werden.« Es ist äußerst fraglich, ob diese AGB wegen ihrer rechtlichen Fehlerhaftigkeit (z.B. die Formulierung »Diese Einwilligung...«) aus materiellrechtlichen Gründen überhaupt Wirksamkeit entfalten kann. Die AGB werden, soweit bisher erkennbar, nicht wirksam in die WM-Ticket-Kunden-Verträge einbezogen. Wegen ihrer Widersprüche zu den AGB des DFB wären sie insofern auch unwirksam.

In den »Datenschutzbestimmungen FIFA Fußball-Weltmeisterschaft 2006« ist die falsche Information enthalten, der RFID-Chip enthalte keine personenbezogene Daten (ebenso Nr. 47 der FAQ). Auf dem Chip werden zwar weder Name noch sonstige Identitätsdaten gespeichert, doch handelt es sich bei der Kennnummer des Chips um ein personenbeziehbares Datum. Durch die Darstellung des DFB kann leicht der Eindruck entstehen, dass auf den Einsatz des RFID-Chips das Datenschutzrecht überhaupt keine Anwendung findet. Dieser Eindruck ist nicht richtig. Über die eindeutige Kennnummer auf dem RFID-Chip werden sämtliche in einer Datenbank des DFB erfassten Antragsdaten erschlossen und sind online abrufbar.

In der Öffentlichkeit wurde vom DFB (OK) die Behauptung verbreitet, die Tickets seien nicht fälschbar, weil jeder Chip weltweit eine fortlaufende Nummer bekommt und deshalb einma-

lig sei.[4] Diese technische Aussage kann vom ULD derzeit nicht verifiziert werden. Falsch ist aber, dass wegen der Einmaligkeit der RFID-Nummer eine Fälschung nicht möglich sei. Mit Hilfe einer Chipkopie ist es in jedem Fall möglich, vor dem tatsächlich Berechtigten das Stadion zu betreten. Es bedarf weiterer Untersuchungen, inwieweit durch zusätzliche Datensicherheitsmaßnahmen Vorkehrungen gegen Fälschungen, also das Kopieren der RFID-Chip-Nummern getroffen wurden.

Die Problematik der RFID-Technologie besteht darin, dass die Transponder-Chips, so die Angaben des DFB, noch aus einer Entfernung von 10 cm unbemerkt ausgelesen werden können. Wer also Zugriff auf die DFB-Ticket-Datenbank hat und die Chips ausliest, kann genau zuordnen, wer der Berechtigte für die Karte ist und wo sich der jeweilige Mensch gerade aufhält. Wäre an jedem Sitzplatz im Stadion ein RFID-Leser angebracht, so könnte präzise lokalisiert werden, welcher Fußball-Fan auf welchem Platz sitzt und auch, wann er - z.B. aus Begeisterung - von seinem Platz aufgesprungen ist. Technisch überprüft werden sollte, ob durch leistungsfähigere Lesegeräte ein Auslesen auch aus einer größeren Entfernung möglich ist.

Gemäß Nr. 51 der FAQ werden die Daten für die Zugangskontrolle im Oktober 2006 nach der Weltmeisterschaft gelöscht. Die Bestellungsdaten richten sich nach den gesetzlichen Aufbewahrungsfristen für solche Papiere (nach Steuerrecht bzw. Handelsgesetzbuch). Keine Angaben machen die vorliegenden Unterlagen zu der Löschung der Daten von denjenigen Ticket-Bestellern, die beim Verkauf nicht berücksichtigt wurden. Diese Daten müssten nach Datenschutzrecht nach Ende der jeweiligen Verkaufsphase gelöscht werden, soweit die Daten nicht mehr für die Vergabe von Tickets benötigt werden (§ 35 Abs. 2 BDSG). Hieran ändert auch die Einwilligung zur Nutzung der Daten für Werbezwecke nichts, da gemäß den obigen Ausführungen diese Einwilligungserklärungen rechtswidrig und daher unwirksam sind.

Eine geradezu satirefähige Formulierung enthält schließlich Nr. 8 der Allgemeinen Ticket-Geschäftsbedingungen. Dort heißt es: »Jeder Ticketinhaber willigt unwiderruflich und für alle gegenwärtigen und zukünftigen Medien ein in die unentgeltliche Verwendung seines Bildes und seiner Stimme für Fotografien, Live-Übertragungen, Sendungen und/oder Aufzeichnungen von Bild und/oder Ton, die vom OK oder dessen Beauftragten in Zusammenhang mit der Veranstaltung erstellt werden«. Die AGB dürfte aus mehreren Gründen unwirksam sein. Dies dürfte aber keine Rolle spielen, da auch bei Unwirksamkeit dieser Klausel praktisch keine Einschränkungen für die Presse-, Funk- und Fernsehberichterstattung entstehen. Insofern haben die Medien aus eigenem Recht die notwendigen Befugnisse. Es ist nicht zu vermuten, dass an jedem Platz eine Kamera und ein Mikrophon installiert wird, mit denen der Zuschauer für mediale Zwecke überwacht wird. Die AGB würden dies erlauben. Was die darin verwendete Formel zeigt, ist etwas anderes: Die kommerzielle Vermarktung scheint dem DFB (OK) wichtiger zu sein als die Rechte seiner Kundinnen und Kunden.

[4] so z.B. SZ 25.01.2005, 33

Bundesverband der Verbraucherzentralen erreicht Änderung der WM-Ticket-AGB

Nachdem der Bundesverband der Verbraucherzentralen (vzbv) den DFB wegen des Bestellformulars sowie der Ticket-AGB abgemahnt hat, wurden diese nun geringfügig geändert.

Beanstandet hatte der vzbv, dass der Eindruck erweckt werde, der Fußballfan müsse der Verwendung seiner Daten für Werbezwecke zwingend zustimmen. Kritisiert wurde außerdem die Einwilligung in die Verwendung von Bildern der Fans sowie die Regelungen für die Preisrückerstattung bei Verlegung eines Spieles.

Damit zeigen sich auch die Grenzen einer Abmahnung nach dem Wettbewerbsrecht, denn die wesentlichen Kritikpunkte konnten nicht berücksichtigt werden.

Es ist weiterhin nicht nachvollziehbar, warum überhaupt eine vollständige Personalisierung der Stadionbesucher erfolgen muss. Dabei wird ein Übermaß an Daten erhoben; an wen diese Daten ggf. weitergegeben werden und wann sie vielleicht doch gelöscht werden, bleibt unklar.

Insofern ist auch nicht verständlich, warum der vzbv nun zusammen mit dem DFB eine Presseerklärung unter dem Titel »Interessen der Fußballfans als Verbraucher müssen im Vordergrund stehen« herausgibt. Die Interessen der Fußballfans werden weiterhin hinter den Überwachungsgelüsten des DFB zurückstehen. *(rs)*

Gemeinsame Erklärung des Verbraucherzentrale Bundesverbands und des FIFA-Fußball-Weltmeisterschaft 2006-Organisationskomitees Deutschland

17.02.2005 - Der Verbraucherzentrale Bundesverband und das OK FIFA WM 2006 haben sich auf eine Klarstellung der Allgemeinen Ticket-Geschäftsbedingungen (ATGB) für die FIFA WM 2006(tm) geeinigt. "Wir stimmen in dem gemeinsamen Ziel überein, dass die Interessen der Fußballfans als Verbraucher im Vordergrund stehen müssen", erklärte OK-Vizepräsident Dr. Theo Zwanziger. "In einem konstruktiven Gespräch haben wir eine übereinstimmende Interessenlage festgestellt," sagte vzbv-Vorstand Prof. Dr. Edda Müller. Bei einem Treffen in Berlin wurden am Donnerstag die in den vergangenen Tagen diskutierten Punkte zur Sprache gebracht.

- In Bezug auf die Ton- und Bildberichterstattung aus den Stadien wird in den ATGB klargestellt, dass die im Kunsturhebergesetz festgelegten Persönlichkeitsrechte der Zuschauer beachtet werden.
- Im Falle der Verlegung eines Spiels erhält der Ticketinhaber die Möglichkeit, die Tickets vor dem Spiel zurückzugeben, und den Ticketpreis erstattet zu bekommen; eine nähere Prüfung der Gründe wird nicht stattfinden. Die ATGB werden entsprechend klargestellt. Zur Übertragung von Tickets ist die Zustimmung des Organisationskomitees notwendig, die, wie in den ATGB bereits vorgesehen, nur in Ausnahmefällen, zum Beispiel aus Sicherheitsgründen, verweigert wird.
- Für den Fan muss eindeutig klar sein, dass eine Ticketbestellung auch dann wirksam wird, wenn er der Verwendung seiner Daten zu Werbezwecken nicht zustimmt. Deshalb wird das Bestellformular an dieser Stelle optisch noch eindeutiger gestaltet.

Diskussion

Auf aussichtslosem Posten - der betriebliche Datenschutzbeauftragte?

Die meisten Unternehmen mit mehr als fünf Arbeitnehmern müssen einen betrieblichen Datenschutzbeauftragten ernennen. Viele haben keinen; oftmals ist er nur Nennbeauftragter, ohne ausreichende Fachkenntnisse und ohne Zeitbudget. Dass er tatsächlich tätig wird, ist weder vorgesehen noch erwünscht. Versucht er dennoch, seine gesetzlichen Aufgaben wahrzunehmen, muss er schnell seine Grenzen erkennen: verweigern Geschäftsleitung und für die Datenverarbeitung verantwortliche Fachbereiche die Zusammenarbeit, ist er praktisch handlungsunfähig.

Der Idealfall, dass eine Unternehmensführung den Datenschutz ernst nimmt und den Datenschutzbeauftragten als wertvollen Garanten dieser Politik sieht und ihn entsprechend unterstützt, ist leider nicht die Regel.

Manfred von Reumont und Rainer Scholl untersuchen in ihren Aufsätzen die Situation des betrieblichen Datenschutzbeauftragten und zeigen Möglichkeiten zur Verbesserung seiner Position auf.

Weitere Artikel und Leserbriefe zu diesem Thema sind erwünscht.

Manfred von Reumont*

Inhaltliche und formale Mängel in DSB-Bestellungen

Ein Plädoyer für optimalen Datenschutz in Betrieben...
... und ein Appell an Geschäftsführer, die betriebliche DSB zu bestellen haben.

»Hiermit bestelle ich Sie mit Wirkung vom ... zum DSB unserer Firma. Ihre Aufgaben ergeben sich aus dem BDSG. Ich bitte um vertrauensvolle Zusammenarbeit in Datenschutzangelegenheiten. Mit freundlichen Grüßen Die Direktion.«

So oder so ähnlich lesen sich manche Bestellungen nach § 4 f (1) BDSG sowohl in der Praxis als auch in etlichen Mustern einschlägiger Fachliteratur und Loseblattsammlungen zum Datenschutz (übrigens: auch die Formulierungsvorschläge auf das Datenschutzgeheimnis fallen ähnlich dürftig aus!).

Diesbezügliche Fragestellungen im Diskussionsforum des virtuellen Datenschutzbüros des Bundesbeauftragten und der LfD[1] als auch Beratungsanfragen interner, betrieblicher Datenschutzbeauftragter (DSB) in Zugleichfunktion machen deutlich, dass o.a. Formulierung oder ähnliche den ohnehin begrenzten Handlungsspielraum eines DSB noch weiter einschränken und beinahe täglich zu Kompetenzstreitereien führen, in der Praxis also wenig hilfreich sind.

Substantielle Aufgabendefinition

Schon die Formulierung »ergeben sich aus dem BDSG« ist zu beanstanden: Per BDSG ergeben sich lediglich die Aufgaben aus § 4 d (6) BDSG, nämlich die Vorabkontrolle, und aus § 4 g BDSG die Hinwirkungspflicht, das Anfragerecht, die Aufgaben der Überwachung der Anwendungen und die Schulung der Verarbeiter, die Ansprüche auf Unterrichtung und auf die Übersicht sowie die Verpflichtung, die Inhalte der Meldepflicht verfügbar zu machen.

Seine im Gesetz zugewiesenen Hauptaufgaben entfallen bei einer Nichtbestellung und sind bei nichtbestelltem DSB unter der verantwortlichen Stelle zu subsumieren. Gerade diesen Sachverhalt wollen manche Firmenleitungen nicht wahrhaben.

Die genannten Funktionen sind allerdings keine eigenverantwortlichen Aufgaben!

So gibt die Hinwirkungspflicht aus § 4 g BDSG dem DSB keinerlei Befugnis, außerhalb der eng begrenzten Aufgaben aus dem BDSG gegen den Willen der Betriebsleitung oder selbständig Maßnahmen im Betrieb umzusetzen bzw. selbständig zu veranlassen; die kreative Eigeninitiative wird abgewürgt. Die »Sicherstellungspflicht« bleibt bei der verantwortlichen Stelle, die nicht an sein Votum gebunden ist[2]. Die Hinwirkungspflicht ist also keine Handlungsermächtigung, die den DSB in die Lage versetzt, selbständig Maßnahmen anzuordnen und durchzusetzen.

Auch am Beispiel der Verpflichtung auf das Datengeheimnis (§ 5 BDSG) wird deutlich, dass die im BDSG dem DSB zugewiesenen Aufgaben einer Auskleidung bedürfen: Wer ist für die Verpflichtung zuständig und verantwortlich? Der Geschäftsführer? Der Leiter der Personal-, der EDV- oder der Rechtsabteilung? Während Schaffland/Wiltfang grundsätzlich den Inhaber oder Geschäftsführer bzw. den Vorge-

* www.mvr-datenschutz.de

1 vpo-datenschutz-list@datenschutz.de

2 Gola/Schomerus, BDSG-Kommentar, Rd.-Nr. 2 zu § 4g BDSG

§ 4f BDSG: Beauftragter für den Datenschutz

(1) [...]

(2) Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Mit dieser Aufgabe kann auch eine Person außerhalb der verantwortlichen Stelle betraut werden. Öffentliche Stellen können mit Zustimmung ihrer Aufsichtsbehörde einen Bediensteten aus einer anderen öffentlichen Stelle zum Beauftragten für den Datenschutz bestellen.

(3) Der Beauftragte für den Datenschutz ist dem Leiter der öffentlichen oder nichtöffentlichen Stelle unmittelbar zu unterstellen. Er ist in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Die Bestellung zum Beauftragten für den Datenschutz kann in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuches, bei nichtöffentlichen Stellen auch auf Verlangen der Aufsichtsbehörde, widerrufen werden.

(4) Der Beauftragte für den Datenschutz ist zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird.

(5) Die öffentlichen und nichtöffentlichen Stellen haben den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen. Betroffene können sich jederzeit an den Beauftragten für den Datenschutz wenden.

§ 4g BDSG: Aufgaben des Beauftragten für den Datenschutz

(1) Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin. Zu diesem Zweck kann sich der Beauftragte für den Datenschutz in Zweifelsfällen an die für die Datenschutzkontrolle bei der verantwortlichen Stelle zuständige Behörde wenden. Er hat insbesondere

1. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten,

2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen.

(2) Dem Beauftragten für den Datenschutz ist von der verantwortlichen Stelle eine Übersicht über die in § 4e Satz 1 genannten Angaben sowie über zugriffsberechtigte Personen zur Verfügung zu stellen. Im Fall des § 4d Abs. 2 macht der Beauftragte für den Datenschutz die Angaben nach § 4e Satz 1 Nr. 1 bis 8 auf Antrag jedermann in geeigneter Weise verfügbar. Im Fall des § 4d Abs. 3 gilt Satz 2 entsprechend für die verantwortliche Stelle.

(3) [...]

setzten des zu Verpflichtenden[3] benennt, belässt es Gola/Schomerus bei dem Hinweis auf die interne Organisation; »bei kleineren Betrieben bietet es sich jedoch an, dem betrieblichen DSB diese Aufgabe zusätzlich zu übertragen«[4] – eine für den DSB unbefriedigende Zuständigkeitsregelung.

Der Leser wird mir zustimmen, dass der Verpflichtende nur der DSB sein kann, zumal ihm die Schulungsaufgabe, deren wesentlichen Inhalte auf das Datengeheimnis hinauslaufen, wiederum expressis verbis obliegt. Wo aber ist die erforderliche Handlungsermächtigung, die die Durchführung der Verpflichtung konkret dem DSB zuweist, auf die er sich berufen kann und dann auch durch ihn durchsetzbar ist?

Da auch andere Aufgaben des BDSG nicht personalisiert sind, sollte eine konkrete Aufgabenzuweisung Bestandteil der förmlichen DSB-Bestellung und damit eine klare Handlungsermächtigung sein. Dadurch werden spätere Auslegungsdebatten vermieden, der Handlungsspielraum des DSB klar definiert und eindeutige Verantwortlichkeiten geschaffen.

So könnten zunächst die allgemeinen Aufgaben mit »...alle Aufgaben, die dem DSB sowie dem Betrieb als nicht-öffentliche Stelle bzw. als verantwortliche Stelle durch BDSG oder bereichsspezifische Vorschriften zugewiesen sind« definiert werden. Und schon ist auch die Datenschutzverpflichtung nach § 5 BDSG eindeutige Aufgabe des bestellten DSB und nicht der Personalabteilung! Oder der DSB ist der zuständige und verantwortliche Vertreter des Unternehmens bei einer Kontrolle der Aufsichtsbehörde.

Mängel und Empfehlungen

■ Immer wieder werden DSB ins kalte Wasser geworfen und ohne jede Fachkunde bestellt, obwohl die Fachkunde eine der Voraussetzungen für die Bestellung (§ 4 f (2) BDSG) ist. Wer aber Verantwortung übertragen bekommt, muss auch in die Lage versetzt werden, diese wahrzunehmen!

Daher muss in der Bestellung der Zeitpunkt des Wirksamwerdens festgelegt werden; damit wird einerseits dem Gesetz Genüge getan und andererseits gewinnt der DSB Zeit für die Aneignung seines Fachwissens. Ein Zeitraum von sechs Monaten scheint mir angemessen zu sein.

■ Unterstützungsmaßnahmen nach § 4 f (5) BDSG müssen konkret formuliert werden, z.B. Etathöhe, Hilfskraft für Schreibarbeiten mit Einsatzzeiten, Ausstattung wie z.B. zusätzlicher stand-alone-Rechner, Mitgliedschaft in einer Datenschutzvereinigung, Abo von Fachzeitschriften usw.

In der Regel kann der DSB bei Beginn seiner Tätigkeit noch nicht den Umfang erforderlicher Hilfe übersehen. Daher bietet es sich an, einen Termin für die Vorlage erforderlichen Bedarfs etwa sechs Wochen nach Bestellungsdatum festzulegen.

■ Zeitlich ähnlich sollte der Aufbau eines Datenschutzmanagements (DSM) geregelt sein. Nach Einarbeitung, Gewinnung eines Überblicks und Analyse der vorhandenen und noch fehlenden Datenschutzmaßnahmen erstellt der DSB eine Planungsgrundlage, in der die erforderlichen Datenschutzmaßnahmen aufführt und einen abge-

[3] Schaffland/Wiltfang, Kommentar BDSG, Rd.-Nr. 19 zu § 5 BDSG

[4] Schaffland/Wiltfang, Rd.-Nr. 13 zu § 5

stimmten Umsetzungszeitplan enthält.

■ Bei einer Zugleichbestellung wird häufig ein Prozentsatz der Gesamtarbeitszeit für die Tätigkeit als DSB festgelegt. Eine solche Größe ist weder einhalt- noch für DSB oder Arbeitgeber kontrollierbar. Besser ist es, Arbeitstage oder Teile davon festzulegen, z.B. DO nachmittag und/oder FR vormittag für ständige und ausschließliche DSB-Aufgabenerledigung, Sprechstunden für Mitarbeiter und Schulungen.

Hier muss auch festgelegt werden, welche bisherigen originären Aufgaben in welchem Umfang an welche Mitarbeiter übertragen werden, damit die Zweitfunktion überhaupt zeitlich ausgeführt werden kann. Es soll ja Leute geben, die sagen, ein DSB habe eigentlich einen fulltime-job ...!

Gleichzeitig muss auch bei zusätzlicher DSB-Tätigkeit (z.B. Vorbereitung einer Prüfung durch die Aufsichtsbehörde oder Einführung eines neuen Verfahrens, wo ein halber Tag in der Woche nicht ausreichen kann) die begrenzte Freistellung von originären Aufgaben festgelegt werden.

■ Eine etwas umfangreichere Definition erfordern die Angaben für den Tätigkeitsbericht und dessen Gliederung, z.B.

- Datenschutzstatus des Unternehmens, vorgegebene Ziele für den Berichtszeitraum
- erfolgte Erledigung der vorangegangenen Zielsetzungen, vorhandene Risikofelder und Probleme, Möglichkeiten der Minimierung oder Beseitigung
- Auswertung der abonnierten mailing-Listen
- Vorschläge zur weiteren Optimierung/Aktualisierung des DSM im Betrieb
- technische Systeme und Datensicherheit (ggfs. durch Leiter EDV)
- Arbeitnehmerdatenschutz: Stand der Mitarbeiterschulung und Verpflichtungen, Beschwerden und deren Erledigung, eigene Fort-/Weiterbildung (!)
- Mängel und Beanstandungen (!) einschließlich Haftungsrisiko bei Nichterledigung
- Vorschläge und Zieldefinitionen für den nächsten Berichtszeitraum

Beispiel: »Mindestens einmal jährlich legt der DSB einen Tätigkeitsbericht über den datenschutzrechtlichen Status der Firma, vorhandene Risikofelder mit Möglichkeiten ihrer Minimierung oder Beseitigung sowie Vorschläge zur weiteren Verbesserung und Aktualisierung datenschutzrechtlicher Belange vor. Hierbei sind außerbetriebliche Weiterentwicklungen im Datenschutzrecht, die einschlägige Rechtsprechung und die zu erwartende Novellierung des BDSG zu beobachten und in den Bericht einfließen zu lassen.«

Ich rate dringend zur (nicht vorgeschrieben) Veröffentlichung des Tätigkeitsberichts in der Firma – schon des Transparenzgebotes wegen! Der Datenschutz und dessen Durchführung gewinnt dadurch in der Firma einen hohen Stellenwert!

■ Dem DSB muss weiterhin eingeräumt werden,

- sowohl interne (Admin, Revision, EDV...) als auch externe Beratung in Anspruch nehmen zu können (ggfs. Begrenzung des Ausgabenvolumens),
- bei der Auswahl ihm zuarbeitender DS-Koordinatoren (z.B. als »KonzernDSB«) in Unternemensverbünden mit entscheiden zu können,
- selbständig Maßnahmen des Datenschutzes (verbindliche Richtlinien, Einweisungen, Beschaffungen) eigenverantwortlich veranlassen und
- über einen festgelegten Etat (Beschaffung Fachliteratur, spezifische Arbeitsmittel usw.) selbständig verfügen zu können.
- Auch die Festlegung von Schulungsumfang, –rhythmen und deren Nachweis gehört in die Kompetenz des DSB und sollte ihm schriftlich zugewiesen werden wie auch
- ein Vortragsrecht (»Aktuelles im Datenschutz«) bei Betriebsversammlungen u. ä.

■ In einer guten Bestellung ist auch die Vertreterregelung und die Vertretung der Firma gegenüber der Aufsichtsbehörde enthalten. Dazu gehört im Vorfeld das selbständige Aufnehmen und Halten der Verbindung mit dieser und anderen Behörden.

■ Die Anrufung der Aufsichtsbehörde, die in öffentlichen Stellen mit der Behördenleitung abzustimmen ist, sollte, außer bei allgemeinen Anfragen, bei nicht-öffentlichen Stellen im Ablauf geregelt sein. Einerseits wird dadurch eine Kollision mit der Treuepflicht als Arbeitnehmer vermieden, andererseits kann eine vorherige Orientierung der Firmenleitung über den beabsichtigten Schritt bei der Bewältigung des vorliegenden Konflikts für beide Seiten hilfreich sein.

In der Praxis hat sich als vorteilhaft erwiesen, in Fällen einer Nichteinigung in der Regelung eine Frist festzuschreiben, binnen derer der DSB die Aufsichtsbehörde anzurufen hat. Eine letzte Besinnungsfrist ...

■ Schließlich soll eine Regelung der Zeichnungsbefugnis nach außen, soweit nicht in einer Geschäftsordnung enthalten, definiert sein. Dies fördert zum einen die wichtigen Kontakte des DSB, entlastet andererseits die Geschäftsleitung.

Form

Es ist unerheblich, in welcher Form die Handlungsermächtigung erfolgt. Sie kann unmittelbarer Bestandteil der Bestellung oder einer Geschäftsordnung, aber auch Inhalt einer gesonderten Stellenbeschreibung sein, die dann aber Bestandteil/Anlage der Bestellung sein muss. Da ein Mitarbeiter zur Annahme der Bestellung nicht verpflichtet ist, sollte die Annahme förmlich erklärt und durch Unterschrift bestätigt werden. Dies beugt späteren »Ausreden« (»Ich wollte ja gar nicht, musste aber...«) bei der Feststellung und Ahndung von Verantwortlichkeiten bei fehlerhaftem Handeln vor.

Fazit

Je allgemeiner und kürzer eine Bestellung ist, um so mehr muss ein DSB um die praktische Ausgestaltung seiner Funktion täglich kämpfen. Dies bindet erhebliche Energien und Resourcen, die woanders im Unternehmen fehlen. Daher liegt eine umfassende, der genannten Mängelliste positiv entsprechende Beauftragung nicht nur im Interesse des DSB, sondern auch und gerade im Interesse der Geschäftsleitung sowie den weiteren Beteiligten im Betrieb (BR, EDV, Recht, Admin usw.).

Je ausführlicher, detaillierter und differenzierter die Funktionen des DSB definiert sind, um so größere, vor allem selbständige Gestaltungsvielfalt und –möglichkeiten (ohne spätere Diskussionen über die Auslegung seiner Beauftragung) hat der DSB bei der täglichen Umsetzung und Verwirklichung des Datenschutzes in seiner Firma.

Persönlichkeit, kooperativer Führungsstil und Vertrauen der Firmenleitung sind Elemente, die eine selbständige und verantwortungsbewusste Zusammenarbeit im Betrieb prägen. Fallen die Faktoren positiv aus, fördern sie bei einem optimal bestellten DSB Leistungsfreude und Selbständigkeit - zum Wohle der Firma und des Grundrechts auf informationelle Selbstbestimmung!

Rainer Scholl

Betriebliche Datenschutzbeauftragte - (un)bedeutend wie der Datenschutz

Der betriebliche Datenschutzbeauftragte hat als Organ der betrieblichen Selbstkontrolle gemäß den gesetzlichen Vorgaben zwei Hauptaufgaben. Zunächst muss er die Entscheidungsträger im Unternehmen in datenschutzrechtlichen Fragen beraten sowie die Mitarbeiter schulen. Außerdem obliegt ihm die Kontrolle der Einhaltung der datenschutzrechtlichen Vorgaben bei der Datenverarbeitung.

Die Motivation der Unternehmen, einen Datenschutzbeauftragten zu ernennen, resultiert zunächst aus der gesetzlichen Verpflichtung[1]. Die Bereitschaft, dem Datenschutzbeauftragten dann auch im erforderlichen Umfang von übrigen Tätigkeiten freizustellen und die notwendigen Mittel zu bewilligen, ist abhängig von deren Einstellung zum Datenschutz.

In vielen Unternehmen dürfte eine pragmatische Einstellung unter Kosten-Nutzen-Überlegungen vorherrschen: Tatsächlich ist für Außenstehende i.d.R. völlig intransparent, welche Datenverarbeitungen in einem Unternehmen stattfinden. Externe Kontrollen sind angesichts der schwachen personellen Ausstattung der Aufsichtsbehörden kaum zu befürchten. Mögliche Sanktionen, so zeigen die Berichte der Aufsichtsbehörden, sind finanziell unbeachtlich. Wenn auch das Risiko strafrechtliche Konsequenzen als gering eingeschätzt wird, wird man sich mit einem »Nennbeauftragten« für den Datenschutz zufrieden geben.

Für einen ernannten Datenschutzbeauftragten, der tatsächlich seine gesetzliche Aufgabe wahrnehmen will, sind damit denkbar schlechte Voraussetzungen gegeben. Er muss sich zunächst das erforderliche Fachwissen aneignen, für Schulungsmaßnahmen wird man ihm aber kaum Mittel bewilligen. Versucht er dann, seine Kontrollaufgabe wahrzunehmen, kann er nicht mit positiver Resonanz rechnen. Ist er, wie meistens, nur ein Teilzeit-Datenschutzbeauftragter, wird er sich überlegen, ob es für ihn nicht besser ist, den Erwartungen gerecht zu werden und seine Aufgabe möglichst nicht wahrzunehmen. Nach dem Gesetz ist er zwar in der Ausübung seiner Fachkunde an keinerlei Weisungen gebunden[2]. Auch darf er nicht wegen der Erfüllung seiner Aufgaben benachteiligt werden[3]. Dennoch ist er nicht wirklich unabhängig, er kann auf vielfältige Weise in seiner Arbeit behindert oder unter Druck gesetzt werden.

Von sich aus hat er kaum Möglichkeiten, eine Besserung der Situation zu erreichen. Bemühungen, eine detailliertere Aufgabenbeschreibung und die Festlegung von Unterstützungsmaßnahmen seitens des Unternehmens zu erreichen, wie von Manfred von Reumont in seinem Artikel in dieser Dana vorgeschlagen, werden ihm kaum weiterhelfen, wenn seine Tätigkeit nicht gewollt ist. Er wird mit solchen Wünschen auf Unverständnis stoßen oder aber formale Vereinbarungen erzielen, deren tatsächliche Inanspruchnahme für ihn nicht ohne Sanktionsrisiko möglich ist. Nur wenn ohnehin eine positive Einstellung zu seiner Tätigkeit vorhanden ist, werden detailliertere Vereinbarungen für eine reibungslosere Arbeit sorgen.

Dem DSB seitens des Gesetzgebers weitgehende Befugnisse und Weisungsrechte hinsichtlich der Datenverarbeitung einzuräumen und ihm die Verantwortung für die Sicherstellung der Einhaltung der datenschutzrechtlichen Vorschriften zu geben, ist nicht zielführend. Da er nicht wirklich unabhängig ist und keinen absoluten Schutz vor Benachteiligung und Kündigung genießt, könnte er diese Verantwortung kaum tragen. Außerdem würde damit auch die Trennung von Verantwortung und Kontrolle unterlaufen.

Sinnvoll erscheint zunächst die Festschreibung dedizierter Anforderungen an das Fachwissen eines betrieblichen DSB durch Gesetzgeber oder Aufsichtsbehörden. Eine obligatorische Prüfung und Zulassung kann die Qualifikation eines Beauftragten sicherstellen.

Unabdingbar ist ein Kündigungsschutz für den Beauftragten vergleichbar dem anderer Funktionsträger wie z.B. dem Immissionsschutzbeauftragten, Abfallbeauftragten oder Betriebsräten.

Hilfreich wäre außerdem, die Störung oder Behinderung der Tätigkeit des Datenschutzbeauftragten analog § 119 BetrVerfG als Straftatbestand einzustufen.

Denkbar wäre auch eine Haftung des DSB für vernachlässigte Prüfungspflichten. Dann wäre kaum noch jemand bereit, sich nur zum »Nennbeauftragten» ernennen zu lassen. Damit würde in den Unternehmen auch das Verständnis für einen DSB, der seine Tätigkeit Ernst nimmt, steigen.

Maßnahmen zur Verbesserung der Position des DSB sollten aber nicht nur an seiner Person ansetzen. Dringend erforderlich ist auch, die Motivation der Unternehmen zu fördern, den Datenschutz Ernst zu nehmen.

Wünschenswert wäre eine drastische personelle Stärkung der Aufsichtsbehörden. Die Anzahl anlassunabhängiger Kontrollen muss soweit gesteigert werden, dass aus Unternehmenssicht eine Kontrolle nicht mehr wie heute unwahrscheinlich ist. Prüfungsumfang und -tiefe dieser Kontrollen müssen dabei erhöht werden.

Wie die Tätigkeitsberichte der Aufsichtsbehörden zeigen, verhängen diese nur äußerst ungern Bußgelder. Sie begnügen sich meistens mit einer Ermahnung und dem Nachweis, dass eine illegale Verarbeitungspraxis geändert wurde. Für die Unternehmen stellt die-

1 § 4f (1) BDSG

2 § 4f (3) S. 2 BDSG

3 § 4f (3) S. 3 BDSG

se Praxis geradezu eine Ermunterung dar, ohne Rücksicht auf die Gesetzeslage zu verfahren. Werden sie erwischt, was eher unwahrscheinlich ist, müssen sie ihre Praxis eben ändern, negative Folgen sind kaum zu erwarten. Erforderlich ist hingegen, dass die Aufsichtsbehörden Datenschutzverstösse konsequent und in ernstzunehmender Größenordnung sanktionieren.

Weiterhin müssen die Betroffenen in ihren Möglichkeiten, ihre Rechte gegenüber den verantwortlichen Stellen wahrzunehmen, gestärkt werden. Erforderlich ist dazu zunächst die Verbesserung der Transparenz, welche Verarbeitungen mit ihren Daten überhaupt stattfinden. Die größtenteils sorglose Einstellung der Bevölkerung zu Fragen des Umgangs mit ihren Daten dürfte darin begründet liegen, dass ihr mangels Transparenz gar nicht bewusst ist, welche Ausmaße die Erhebung, Verarbeitung und Weitergabe ihrer personenbezogenen Daten bereits angenommen und welche Folgen dies für sie hat oder noch haben kann.

Erst bei ausreichender Transparenz kann sich der Datenschutz als Wettbewerbsfaktor entwickeln. Der Verbraucher kann den Umgang mit seinen Daten als Kriterium für seine Konsumentscheidungen einbeziehen.

Wichtig ist die Transparenz nicht nur für die Betroffenen, auch den Wettbewerbern sollte die Möglichkeit gegeben werden, wirtschaftliche Vorteile ihrer Konkurenten, die diese durch Datenschutzverstöße erlangen, zu erkennen und als wettbewerbswidriges Verhalten abmahnen und unterbinden zu können.

Um die betriebliche Selbstkontrolle durch den Datenschutzbeauftragten und damit die Durchsetzung des Datenschutzes zu fördern, müssen die richtigen Rahmenbedingungen gesetzt werden, damit alle Akteure, der DSB, die hoheitlichen Aufsicht, die Betroffenen sowie die Marktteilnehmer auf die datenverarbeitenden Unternehmen einwirken können.

Der Datenschutzbeauftragte wird erst dann in den Unternehmen Ernst genommen, wenn auch der Datenschutz unverzichtbarer Bestandteil einer erfolgreichen Unternehmensstrategie geworden ist.

Bundesdruckerei gewinnt CCCeBIT-Award für die Forcierung biometrischer Reisepässe mit RFID

CCC: Biometrische Merkmale in Ausweisdokumenten sinnlos, gefährlich, teuer

Für ihre Lobbyarbeit und das gekonnte Ignorieren technischer Probleme in Sicherheits- und Datenschutzfragen vergab der Chaos Computer Club auf der diesjährigen CeBIT den CCCeBIT-Award an die Bundesdruckerei.

Auf 670 Millionen Euro veranschlagt das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) die erstmaligen Investitionskosten für die Einführung von Ausweisen mit Speicherchips, die laufenden jährlichen Kosten werden auf 610 Millionen Euro geschätzt. Diese erwarteten Umsätze sieht der CCC als Motiv für den ehemaligen Staatsbetrieb, trotz des nicht erwiesenen Sicherheitsgewinns und der noch nicht ausreichend erprobten Technik die Einführung der RFID-Reisepässe zu forcieren.

Der CCC sieht das ganze Vorhaben als datenschutztechnisch sehr zweifelhaft an:

»1. Bisher hat die Regierung nicht darlegen können, wozu die BRD Biometrie und RFID überhaupt braucht oder wie dadurch ein echter Sicherheitsgewinn entstehen kann. Die Totalerfassung der Bevölkerung bringt keinen Sicherheitsgewinn, schafft aber Risiken und Begehrlichkeiten. Laut BMI und Bundesdruckerei sind schon die bisherigen Personaldokumente praktisch nicht zu fälschen.

2. Viele technische Verfahren zur Erfassung und Erkennung von biometrischen Merkmalen können im Bezug auf den angeblichen Zugewinn an Sicherheit als zweifelhaft bezeichnet werden. So lassen sich mit sehr geringem Material- und Zeitaufwand beispielsweise viele Fingerabdruckscanner überlisten, wie der CCC vorgeführt hat und wie auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) festgestellt hat. [...]

3. Die Wahl von kontaktlosen RFID-Chips zur Speicherung der biometrischen Merkmale in den Ausweisdokumenten bringt das zusätzliche Risiko mit sich, dass ungeschützte Daten vom Ausweisinhaber unbemerkt ausgelesen werden. Das vom Bundesverfassungsgericht aus dem Grundgesetz abgeleitete Recht auf informationelle Selbstbestimmung wurde bei der Auswahl der Technologie offenbar vollständig ignoriert. Selbst wenn das unbemerkte Auslesen der biometrischen Merkmale verhindert werden kann, bleibt das Risiko des drahtlosen Verfolgens mittels versteckter Lesegeräte bestehen.

4. Es ist vollkommen unklar, ob der kryptografische Ausleseschutz von biometrischen Daten vom Reisepass als Datenträger sicher ist. Die bei der internationalen Standardisierung von deutscher Seite aus vorgebrachten sinnvollen Vorschläge zur Verschlüsselung sind für andere Staaten nur optional. Es ist daher davon auszugehen, dass für Bundesbürger im Ausland kein Schutz existiert.

5. Grundsätzliche Fragen über das Verfahren und den Umgang mit den neuen Dokumenten sind ungeklärt: Wer ist schuld, wenn der Tag nicht mehr funktioniert? Ist der Passinhaber dann ein Terrorist? Oder wird der Inhaber dann wie bisher nach optischer Prüfung des Fotos durchgelassen?«

Der CCC fordert daher, auf biometrische Merkmale in Pässen und Ausweisen zu verzichten. Zumindest sollte vor dem Einsatz ein öffentlich begleiteter Feldtest stattfinden, die sensiblen Personendaten dürften nur verschlüsselt abgelegt werden und müssten einer strengen Zweckbindung unterworfen werden. *(rs)*

(www.ccc.de, www.tab.fzk.de)

Datenschutznachrichten

Deutsche Datenschutznachrichten

Bund

Zwei Lagezentren, ein Anti-Terror-Kampf

Entgegen den Vorstellungen von Bundesinnenminister Otto Schily (SPD), aber auch der CDU- bzw. CSU-Landesinnenminister Günther Beckstein (Bayern: »Trauerspiel«) und Uwe Schünemann (Niedersachsen: »Wasserkopf«) gibt es seit dem 14.12.2004 zur Terrorismusabwehr nicht ein gemeinsames Lage- und Analysezentrum, sondern gleich zwei, jeweils eines für die Polizeien und für die Geheimdienste. Anstelle der gemeinsamen Datei sind nun zwei getrennte Dateien geplant, so dass Verfassungsschützer und Polizeien nicht sehen können, über welche Informationen der jeweils andere verfügt. Statt alle Experten an einen Tisch zu setzen, sollen nun sieben Koordinierungsforen die Arbeit von Bundeskriminalamt (BKA) und Bundesamt für Verfassungsschutz (BfV) abgleichen, z.B. die »Große Runde« im BKA und das bisher schon arbeitende »Information Board« zwischen Polizei und Geheimdiensten. In die Koordinierung müssen dann noch die Erkenntnisse des Bundesnachrichtendienstes (BND) einfließen, der weiterhin sein eigenes Lagezentrum im Berliner Süden beibehält. Die beiden Zentren sollen PIAD und NIAD heißen (Polizeiliches bzw. Nachrichtendienstliches Informations- und Analysezentrum). Sie werden in benachbarten Häusern auf dem Gelände des BKA in Berlin-Treptow eingerichtet. Damit bleibe, so eine Sprecherin des Bundesinnenministeriums, das Trennungsgebot zwischen Polizei und Nachrichtendiensten formal gewahrt.

Nach Ankündigung des Bundesinnenministeriums soll es aber tägliche aktuelle Lagebesprechungen geben, bei denen polizeiliche und nachrichtendienstliche Erkenntnisse ausgetauscht werden, Gefährdungsbewertungen, operativen Informationsaustausch zwecks Abstimmung operativer Maßnahmen, Fallauswertungen und Strukturanalysen. PIAD und NIAD werden nicht rund um die Uhr besetzt sein, sondern jeweils von 6 bis 20 Uhr. Das BKA setzt sofort rund 100 Spezialisten ein, das BfV zunächst 15, die bis Mitte 2005 auf 50 aufgestockt werden sollen, der BND 5. Von den 16 Ländern sollen insgesamt 32 Beamte am Info-Austausch teilnehmen. Sachsen, Sachsen-Anhalt, das Saarland und Bremen stellen bisher keine eigenen Fachleute zur Verfügung. In die Arbeitsabläufe eingebunden sein sollen neben BND, BfV, Landesämter für Verfassungsschutz, BKA und Landeskriminalämter sowie der Bundesgrenzschutz (BGS, künftig Bundespolizei, s.u.), das Zollkriminalamt und der Militärische Abschirmdienst (MAD).

Neben dieser organisatorischen Maßnahme will die Bundesregierung für die gemeinsame Arbeit von Polizei und Nachrichtendiensten des Terrorismuszentrums zügig die rechtlichen Voraussetzungen für gemeinsame Projektdateien und eine gemeinsame Index-Datei schaffen (Käppner, Ramelsberger SZ 11./12.12.2004, 4, 6; 15.12.2004, 1, 5; BMI Internetredaktion 21.12.2004 u. 14.12.2004).

Bund

BGS wird zur »Bundespolizei«

Am 19.01.2005 wurde vom Bundeskabinett ein Gesetz beschlossen, mit dem 400 Einzelregelungen in 136 Gesetzen und Verordnungen verändert werden, ohne dass sich tatsächlich irgend etwas direkt materiell ändert: Der Begriff »Bundesgrenzschutz« (BGS) wird durch den Begriff »Bundespolizei« ersetzt. Mit der Umbenennung des BGS soll eine Anpassung des Namens an die Änderung und Ausweitung der Aufgaben erfolgen. Der 1951 begründete BGS erhielt seit den Notstandsgesetzen 1968 immer mehr Aufgaben und Befugnisse. Er übernahm den Küstenschutz, den Objektschutz von Bundeseigentum, die polizeiliche Begleitung bundesweiter Protests, mit der Bahnpolizei den Fahndungsdienst in Zügen und Bahnhöfen sowie die Sicherung von Flughäfen und des Luftverkehrs.

Zwar hatte das Bundesverfassungsgericht auf Klage des Landes Nordrhein-Westfalen im Jahr 1998 die Ausweitung der Kompetenzen zu stoppen versucht, der Ausbau zu einer »multifunktional einsetzbaren Polizei« sei nicht mit dem Grundsatz »Polizei ist Ländersache« vereinbar. Doch darf gezweifelt werden, dass diese Ermahnung politisches Gehör findet. Die Namensänderung wird sich auf viele Stellen auswirken: Das Bundeskriminalamt (BKA) wird zur Bundeskriminalpolizei, der Grenzschutz wird zur Bundesschutzpolizei. Künftig soll es weiterhin ein Bundespolizeipräsidium, ein Bundespolizeiamt, Bundespolizeidirektionen und Bundespolizeiinspektionen geben (Prantl, SZ 20.01.2005, 4).

Bund

BND erhält mehr Abhörbefugnisse

Der Bundesnachrichtendienst (BND) soll nach dem Willen der Bundestagsfraktionen von SPD und Grünen mehr Möglichkeiten beim Abhören von Telefongesprächen erhalten. Gemäß einem gemeinsamen Gesetzentwurf soll der deutsche Auslandsgeheimdienst in besonders wichtigen Fällen auch mutmaßliche Schleuser belauschen dürfen. Das Gleiche gilt für Gespräche, die von Schiffen in internationalen Gewässern geführt werden, wenn Anhaltspunkte für besondere Straftaten vorliegen. Mit der Erweiterung des sog. Jolo-Paragrafen soll der BND zudem besser reagieren können, wenn etwa Deutsche im Ausland entführt werden. Der Gesetzentwurf räumt in diesen Fällen vereinfachte Suchmöglichkeiten zur Identifikation der Verdächtigen ein. Auf der philippinischen Insel Jolo war 2000 u.a. die Göttinger Familie Wallert entführt worden; der BND hatte damals zu Beginn angeblich Schwierigkeiten bei der

Telefonüberwachung gehabt (Der Spiegel 50/2004, 19; vgl. DANA 1/2001, 20 f.).

Bund

Biometrischer Ausweis kostet bis zu 700 Mio. Euro

Gemäß einem Bericht des Büros für Technikfolgenabschätzung beim Deutschen Bundestag (TAB), der am 17.11.2004 vorgelegt wurde, kostet die Einführung von Ausweisen mit biometrischen Merkmalen (Gesicht, Finger, Iris oder Hand) den Steuerzahler bis zu 700 Mio. Euro. Je nach Modell werden die Kosten für die Erstausstattung von 22 Mio. Euro bis rund 700 Mio. Euro prognostiziert, der Aufwand für die jährliche Aktualisierung von rund 4,5 Mio. Euro bis 600 Mio. Euro. Die Grünen-Politikerin Silke Stokar befürchtet, dass der Bürger künftig 130 Euro pro Pass hinblättern muss. Bislang kostet ein Reisepass in Deutschland 26 Euro; wer unter 26 Jahre alt ist, bezahlt 13 Euro.

Auf EU-Ebene sind die politischen und rechtlichen Weichen für eine harmonisierte biometrische Nutzung in Ausweisdokumenten und Visa gestellt. Das deutsche Recht enthält im Ausländerrecht sowie im Pass- und im Personalausweisgesetz entsprechende Regelungen. Europa und Deutschland liegen gemäß dem Bericht in der Umsetzung der Biometrie bei Ausweisen und Visa zurück. Australien gehört zu den 30 Staaten, die nur noch Personalausweise mit biometrischen Gesichtsinformationen der InhaberIn herausgeben. Ägypten stattet seit Januar 2001 seine 42 Mio. BürgerInnen mit ID-Ausweiskarten aus, die einen biometrischen Fingerabdruck enthalten (de.internet.com 17.11.2004; Krüger, Spiegel-online 10.12.2004).

Bund

Verlobte sollen aussagepflichtig werden

Gemäß einer gemeinsamen Gesetzesinitiative von Hamburg und Berlin im Bundesrat sollen Verlobte künftig im Strafverfahren nicht mehr die Aussage verweigern können. Nach Ansicht des hamburger Justizsenators Roger Kusch (CDU) und seiner berliner Kollegin Karin Schubert (SPD) liegt die rechtliche Bedeutung eines Verlöbnisses »schon lange nicht mehr in dem gegenseitigen Heiratsversprechen, sondern in den Zeugnisverweigerungsrechten«. Die Strafprozessordnung schützt Verlobte in gleichem Maße wie Ehepartner und nahe Angehörige. Sie müssen nicht aussagen, körperliche Untersuchungen wie Blutentnahmen nicht dulden und nicht den Briefverkehr mit dem Beschuldigten offen legen. Weil das Verlöbnis an keine Form gebunden ist und nicht öffentlich erfolgen muss, lässt es sich vor Gericht nur schwer überprüfen (Der Spiegel 51/2004, 21; SZ 13.12.2004, 6).

Bund

Bei Kreditkartenverlust einheitliche Notrufnummer

Die Regulierungsbehörde für Post und Telekommunikation (RegTP) hat am 21.12.2004 dem berliner Verein Sperr e.V. den Zuschlag zum Betrieb der ab 01.07.2005 eingeführten einheitlichen neuen Notfallnummer 116116 erteilt. Diese soll, so Bundesinnenminister Otto Schily, »die erste einheitliche Sperrnummer für elektronische Berechtigungen sein«. Gesperrt werden können EC- und Kreditkarten, Mitarbeiterausweise oder das Handy. Will jemand nicht auf den gesamten Kosten beim Missbrauch von abhanden gekommenen Karten oder Handys sitzen bleiben, ist mensch verpflichtet, innerhalb einer kurzen Frist den Verlust zu melden. Wer die einheitliche Nummer wählt, erreicht ein Callcenter, dem er anonym mitteilt, welche Berechtigungen er sperren lassen möchte. Damit soll auch der Datenschutz gewährleistet werden. Die Callcenter-MitarbeiterInnen entnehmen aus ihrer Datenbank eine Liste von Notrufnummern, die der Geschädigte bisher direkt hätte anrufen müssen. Zu diesen Anschlüssen wird der Anrufer dann nacheinander automatisch durchgestellt. Er muss dann allerdings die Nummern der Kreditkarten parat haben. Diese Angaben werden in der Datenbank des Vereins Sperr nicht gespeichert. Dieser übernimmt auch keine Haftung für die Sperrung.

Technisch werden bei dem neuen System sog. Intelligente Netze (IN) eingesetzt, die die Deutsche Telekom betreibt. Sie verbinden den Anrufer mit den Hotlines der Banken und anderer Firmen. Die IN sorgen auch dafür, dass jeder, der innerhalb von 30 Minuten vom gleichen Apparat anruft, wieder zur gleichen Sperr-BeraterIn gelangt. Dies kann sinnvoll sein, wenn z.B. während des Notrufs von einem Handy die Verbindung abreißt. Da die Kontosperrung nur die Banken, Mobilfunkbetreiber usw. selbst vornehmen können, müssen diese an das System angeschlossen werden. Sie müssen auch die Kosten in Höhe von 1,60 Euro pro zu sperrende Karte tragen. Für den Anrufenden muss wegen der RegTP-Auflagen von Deutschland aus die Sperrung kostenfrei sein.

Der Vorsitzende von Sperr e.V., Michael Denck, ist optimistisch, dass die Wirtschaft sich an dem Projekt beteiligen wird. Bertelsmann und Bosch werden in Wilhelmshaven und Magdeburg im Auftrag des Vereins jeweils ein Callcenter betreiben. Eingesetzt werden keine Sprachsysteme, sondern menschliche Gesprächspartner. Der Verbraucherzentrale Bundesverband (vzbv) begrüßt, so Telekommunikationsreferent Michael Bobrowski, das Modell. Es zähle schließlich »jede Minute, um hohe Schäden zu vermeiden«. Wünschenswert sei eine europaweit einheitliche Rufnummer, und es sollte jeweils dokumentiert werden, wann der Kunde anrief. Nach einem EU-Beschluss vom August 2004 soll die 116 in ganz Europa die Basis für Notfallnummern werden (Arzt, SZ 22.12.2004, 11).

Bund

Kontoevidenz verzögert sich

Der automatisierte Abruf von Kontendaten durch die Finanzämter kann voraussichtlich nicht - wie geplant - zum 01.04.2005 in Betrieb gehen. Bei der Umsetzung sind sich die beteiligten Bundesbehörden über wichtige technische Details nicht einig geworden. Gesetzlich ist vorgesehen, dass die Finanzämter und andere Behörden über das Bundesamt für Finanzen (BfF) heimlich auf die Kontendaten jedes Bankkunden in Deutschland Zugriff nehmen können (DANA 4/2004, 25 f.). Beim Bundesverfassungsgericht sind inzwischen zwei Verfassungsbeschwerden hiergegen anhängig, darunter eine von der Volksbank Raesfeld sowie der Antrag auf eine einstweilige Anordnung. Auch der Deutsche Anwaltsverein hält den auto-

DATENSCHUTZ NACHRICHTEN

REGISTER FÜR DEN JAHRGANG 2004

Bearbeitung: Karin Bauer

Register-Inhalt

I. Themenschwerpunkte der einzelnen Dana-Ausgaben

II. Aufsätze

III. Stellungnahmen, Aufrufe, Presseerklärungen

IV. Rechtsprechung

(einfache Datumsangabe ist Datum der Veröffentlichung)

V. Buch- und Broschürenbesprechungen

VI. Deutsche Datenschutznachrichten

Niedersachsen

Nordrhein-Westfalen

Rheinland-Pfalz

Sachsen

Schleswig-Holstein

Thüringen

VII. Ausländische Datenschutznachrichten

Afrika

Brasilien

China

Dänemark

Estland

EU

Frankreich

Georgien

Großbritannien

International

Island

Israel

Italien

Japan

Kuba

Kolumbien

Österreich

VIII. Welt der Technik

IX. Welt der Gentechnik

X. Stichworte

Datenschutz Nachrichten - Jahresregister 2004
Herausgegeben von der Deutschen Vereinigung für Datenschutz e.V. - DVD
Geschäftsstelle: Bonner Talweg 33-35, 53113 Bonn, Tel. 0228-222498, E-Mail: dana@datenschutzverein.de
Bearbeiterin: Karin Bauer — Beilage zur DANA 1/2005

matisierten Kontenabruf für verfassungswidrig.

Der Zentrale Kreditausschuss (ZKA), die Dachorganisation der deutschen Kreditwirtschaft, hält den Einführungstermin nicht mehr für erreichbar. In einem Schreiben des ZKA vom 14.12.2004 an das Bundesfinanzministerium, das diesem unterstellte BfF und die Bundesanstalt für Finanzdienstleistungsaufsicht (BAFin) heißt es: »Wir möchten Sie hiermit erneut darauf aufmerksam machen, dass die Umsetzung der neuen Anforderungen mit einem erheblichen zeitlichen Vorlauf ... verbunden und der gesetzlich vorgesehene Einführungstermin 1. April 2005 aus unserer Sicht nicht mehr einzuhalten ist. ... Insofern bitten wir Sie, den Einführungstermin entsprechend zeitlich zu verschieben«. Eine Vorlaufzeit von mindestens sechs Monaten erscheine angebracht. Hintergrund sind Differenzen zwischen dem BfF und der BAFin über technische Details bei der Umsetzung der Kontenabfrage. Die BAFin kann bereits seit zwei Jahren auf die Datensätze mit den Kundenstammdaten bei den Banken zugreifen. Diese »Kontoevidenzzentrale« wurde im Zuge der Anschläge des 11.09.2001 eingerichtet, um organisierte Geldwäsche und die Finanzsysteme von Terror-Organisationen zu bekämpfen. Mit dem »Gesetz zur Förderung der Steuerehrlichkeit« soll auch das BfF Zugriff auf den Datenpool erlangen. Hierfür bedarf einer Einigung von BAFin und BfF auf eine gemeinsame Schnittstellen-Spezifikation (http://de.internet.com/index.php?id=2033422).

Bund

BfD: ELSTER stoppen

Mit dem Steueränderungsgesetz 2003 vom 15.12.2003 (BGBl. I S. 2645) wurde die Einführung der »elektronischen Lohnsteuerkarte« (ELSTER) ab dem Kalenderjahr 2004 beschlossen. Der Bundesbeauftragte für den Datenschutz (BfD) Peter Schaar hat gefordert, wegen massiver Sicherheitslücken das Verfahren der elektronischen Steuererklärung für Unternehmen vorläufig zu stoppen: »Sollte es das Bundesfinanzministerium nicht schaffen, ein datenschutzrechtlich einwandfreies Verfahren zu gewährleisten, muss die Software so lange abgeschaltet werden«. Firmen sind seit dem 01.01.2005 verpflichtet, Umsatzsteuer- und Lohnsteuererklärungen elektronisch mit Hilfe der ELSTER-Software an das zuständige Finanzamt zu übermitteln. Zur Erstellung einer solchen Erklärung ist nur die Steuernummer nötig. Es wird kein Passwort abgefragt und keine Identifizierung vorgenommen. Damit kann jeder, der die Steuernummer einer Firma kennt, deren Zahlen ändern, ohne dass dies vom Finanzamt kontrolliert wird. Besonders leicht ist der Missbrauch, da seit kurzem die Firmen verpflichtet sind, auf jeder Rechnung ihre Steuernummer anzugeben. Auch der Bund der Steuerzahler (BdSt) fordert, das Sicherheitsloch schnell zu stopfen.

In der Finanzverwaltung sind die Probleme bekannt. Den Unternehmen wird geraten, Abbuchungen des Finanzamtes genau auf Manipulationen hin zu überprüfen und bereits erteilte Einzugsermächtigungen vorsichtshalber zu kündigen. Ein finanzielles Risiko entstehe den Unternehmen jedoch nicht, da die Firmen im Falle unrechtmäßiger Abbuchungen bei ihrer Bank auch telefonisch widersprechen könnten, so dass das Geld auf Kosten des Finanzamtes zurückerstattet werde. Die Finanzverwaltung arbeitet »mit Hochdruck« an einer passwortgeschützten Software. Mit einem Einsatz eines sicheren Systems könne - so ein Vertreter der Finanzverwaltung - jedoch nicht vor Sommer 2005 gerechnet werden (tagesschau.de 16.12.2004; SZ 17.12.2004, 22).

Bund

Informationsfreiheitsgesetz kommt

Der Deutsche Bundestag hat am 17.12.2004 erstmals über einen Entwurf der roten-grünen Fraktionen zu einem Informationsfreiheitsgesetz (IFG) beraten, durch das BürgerInnen, JournalistInnen und Bürgerrechtsverbände künftig wesentlich leichter Akten und Datenbestände der Bundesverwaltung einsehen können. Eine persönliche Betroffenheit muss nicht gegeben sein. SPD-Abgeordneter Michael Bürsch: »Jeder hat dann Anspruch auf amtliche Informationen des Bundes.« Es sind aber Ausnahmen vorgesehen, z.B. wenn eine Offenlegung sich nachteilig auf internationale Beziehungen oder die Kontrollen von Finanzbehörden auswirken könnte. Zuvor hatte der Petitionsausschuss des Bundestags beschlossen, ein IFG einführen zu wollen. In seinem Beschluss stellt er heraus, dass ein IFG zur Stärkung der demokratischen Beteiligungsrechte der BürgerInnen erforderlich sei. Die Praxis aus den Bundesländern, in welchen es bereits Informationsgesetze gibt, widerlege die bisher geäußerten Bedenken wie die Furcht vor einer »Aktenflut«. Ein solches Gesetz könne Transparenz des Verwaltungshandelns herstellen und zur Korruptionsbekämpfung beitragen.

Die Opposition sowie Journalisten- und Bürgerrechtsverbände kritisierten die Gesetzesvorlage als nicht ausreichend. Volker Hummel, stellv. Vorsitzender der Deutschen Journalisten-Verbandes (DJV): »Der Entwurf liest sich stellenweise noch wie ein Gesetz zur Verhinderung der Informationsfreiheit.« Es gebe zu viele Ausnahmen, mit denen sich das Gesetz gleich wieder aushebeln lasse. Christoph Bruch von der Humanistischen Union (HU) assistiert: »Die Auskunftspflicht kann jederzeit unterlaufen werden.« Es müsse daher nachgebessert werden. Grundsätzlich begrüßen aber die Bürgerrechts- und Journalistenverbände das Gesetz. Bruch: »Die Mauer, mit der sich die öffentliche Verwaltung zum Schutz vor Neugier der Bürger umgibt, beginnt zu bröckeln.« Bundesinnenminister Otto Schily (SPD) warnte in der Parlamentsdebatte vor den Risiken von zu viel Offenheit. Zwischen Datenschutz und Auskunftspflicht existiere ein Spannungsfeld. Die Unionsfraktion wünscht sich ebenfalls weitere Einschränkungen. So dürfe es eine Datenfreigabe nur geben, wenn ein berechtigtes Interesse des Bürgers vorliege, sagte die CDU-Abgeordnete Beatrix Philipp (Brychcy, SZ 18./19.12.2004, 6; PM Bündnis 90/Die Grünen Nr. 877 v. 01.12.2004).

Bund

PDS als extremistische Organisation eingestuft

In einer Liste des Bundesamtes für Verfassungsschutz (BfV) wird die Partei des Demokratischen Sozialismus (PDS) neben Terrororganisationen wie al-Qaida, Taliban oder der Neonazi-Gruppe Blood&Honour als »extremistische Organisation« aufgeführt. Es werden mehr als 120 Vereinigungen gelistet. Die Liste wird z.B. einbürgerungswilligen Ausländern vorgelegt, in der Er-

wartung, dass sie sich ausdrücklich distanzieren und statt dessen sog. Loyalitätserklärungen zur freiheitlich-demokratischen Grundordnung abgeben. Obwohl die PDS in zwei Bundesländern an Regierungen beteiligt ist, wäre damit die Mitgliedschaft ein Einbürgerungshindernis. Das Bundesministerium des Innern (BMI) rechtfertigte die Aufnahme der PDS in die Liste mit ihren Kontakten zur kurdischen PKK. Eine kuriose Folge dieser Einstufung ist, dass das Innenministerium Rheinland-Pfalz die Postkommunisten als »extremistische Ausländerorganisation« führt. Der Vorsitzende der PDS, Lothar Bisky, protestierte gegen die Einstufung seiner Partei in einem Schreiben an Innenminister Otto Schily (SPD). Daraufhin wies das BMI das BfV an, die PDS wieder von der Liste zu streichen. Die Aufnahme der PDS auf der zwischen Bund und Ländern abgestimmten Liste war, so das BMI, »auf Antrag eines Bundeslandes« erfolgt. Inzwischen habe sich »die Aufnahme inländischer Organisationen auf diese Liste als nicht zielführend erwiesen«.

Ein weiteres »Extremismusproblem« hat die PDS mit der von ihr seit 1999 als Jugendverband anerkannten Organisation Solid, was für »sozialistisch, links, demokratisch« steht. Solid hat bundesweit ca. 1400 Mitglieder. Nach Einschätzung des BfV wird der »neue Bundessprecherrat von Solid zum Großteil von der eher kommunistisch geprägten Strömung dominiert«. Solid arbeite mit »anderen deutschen Linksextremisten zusammen« und pflege »Kontakte zu ausländischen Linksextremisten«. Während auch in der PDS-Jugend Kritik an der kapitalismuskritischen Organisation geübt wird, beteuert Lars Kleba, stellv. Bundesjugendreferent der PDS, dass die Zusammenarbeit mit Solid sehr gut sei: Solid sei eine »wichtige Vorfeldstruktur« für die Partei. Für viele spiegeln die Probleme des Jugendverbandes die Situation innerhalb der Partei wieder. In dieser selbst gibt es mit der Kommunistischen Plattform und dem Marxistischen Forum Strömungen, die der beamtete Verfassungsschutz als »offen extremistische Kräfte« bezeichnet. Victor Perli, einer der acht Vorstandssprecher von Solid, wehrt sich gegen die Einstufung des BfV, der von einem »traditionell kommunistisch orientierten Flügel« im Jugendverband berichtet: »Das Durchschnittsalter von Solid liegt bei 19 Jahren. Da kann man doch nicht von traditionell kommunistischer Einstellung sprechen.« Der 22jährige spricht dagegen von einem »Staatsapparat« in Deutschland, der nicht akzeptieren könne, dass es links von der Sozialdemokratie noch eine politische Organisation gebe, wie es auch in anderen europäischen Ländern üblich sei (Hummel, SZ 18./19.12.2004, 11; SZ 13,12,2004, 6; Der Spiegel 51/2004, 19).

Bund

Patientenquittungen wenig gefragt

Die Kassenärztlichen Vereinigungen und die Krankenkassen teilten mit, dass die bei der Gesundheitsreform eingeführte Möglichkeit, sich nach dem Arztbesuch die Leistungen quittieren zu lassen, von den KassenpatientInnen kaum genutzt werden. Als Gründe werden fehlende Informationen der PatientInnen sowie geringes Interesse vermutet. Die kostenlose Patientenquittung kann seit Beginn des Jahres 2004 nach jedem Arztbesuch erbeten werden (SZ 10.12.2004, 6; vgl. auch S. 31).

Bund

Managergehälter offenlegen

Das bayerische Kabinett hat am 16.11.2004 beschlossen, im Bundesrat eine Gesetzesinitiative zu starten, die die individuelle Veröffentlichung der Gehälter von Vorständen in Aktiengesellschaften zur Vorschrift macht. Bayern will damit Bundesjustizministerin Brigitte Zypries (SPD) zuvorkommen, die eine ähnliche Initiative für Sommer 2005 plant. Die Ministerin will abwarten, ob genügend Konzerne aus dem Deutschen Aktienindex (Dax) freiwillig ihre Managergehälter publizieren, und erst dann über mögliche Zwangsmaßnahmen entscheiden. Zypries zuvor kommen wollen auch die Fraktionen von SPD und Grüne, die ein entsprechendes Gesetz ankündigten. Die Fraktionsspitzen haben eine Arbeitsgruppe unter Leitung von Ludwig Stiegler (SPD) und Fritz Kuhn (Grüne) beauftragt, einen Entwurf auszuarbeiten. Kuhn: »Schon jetzt haben viele Konzerne erklärt, dass sie die Vorstandsgehälter nicht offen legen wollen. Warum sollen wir da noch warten?«

Im Handelsgesetzbuch (HGB) ist geregelt, dass die Bezüge der Vorstände in angemessenem Verhältnis zur wirtschaftlichen Lage des Unternehmens sowie zur Leistung des jeweiligen Vorstandsmitglieds stehen müsse. Die bayerische Staatsregierung will diese HGB-Regelung »mit Leben füllen«. Der individuelle Gehaltsausweis solle mehr Transparenz v.a. für die Aktionäre schaffen. Hierdurch könne »das Vertrauen der Anleger in den Kapitalmarkt« gestärkt werden. Die Aufsichtsräte börsennotierter Gesellschaften seien in den letzten Jahren ihrer Pflicht, die Vorstandsbezüge auf ein angemessenes und sozialadäquates Maß hin zu kontrollieren, »nicht hinreichend nachgekommen«.

Bisher müssen deutsche Aktiengesellschaften in ihren Geschäftsberichten nur die Summe der Bezüge aller Vorstandsmitglieder ausweisen. Der Verhaltenskodex der Regierungskommission Corporate Gouvernance, der Empfehlungen für die deutsche Unternehmensführung macht, spricht sich auch für den individuellen Gehaltsausweis aus. Ein solcher ist z.B. in den USA und in Großbritannien vorgeschrieben. Nur weniger als die Hälfte der im Dax notierten Unternehmen folgte bisher den Empfehlungen der Kommission, jüngst die Hypo Vereinsbank. Ein Drittel des guten Dutzends an Dax-Unternehmen, die die Bezüge offen legen wollen, haben dies erst in den letzten Monaten angekündigt (SZ 11.01.2005, 21; SZ 17.11.2004, 22, 24).

Bund

Pfizer will Patientendaten gegen Medikamenten-Kostenersatz

Der US-Pharmakonzern Pfizer hat Probleme mit der Gesundheitsreform und den damit verbundenen Arzneipreisregeln. Um seinen zu teuren Blutfettsenker »Sortis« weiterhin zu verkaufen, hatte die Firma die Idee, den Patienten die zusätzlichen Kosten für das Medikament teilweise auf Antrag zu erstatten, ohne aber die Preise für sein Medikament zu senken. Zu der Preissenkung im Bereich der gesetzlichen Krankenversicherung ist Pfizer durch Einstufung von Sortis in eine Festbetragsgruppe seit Anfang 2005 rechtlich verpflichtet. Im Gegensatz zu seinen Konkurrenten hat Pfizer den Preis von Sortis nicht gesenkt, so dass dieses Medikament ein Drittel mehr als

entsprechende Produkte anderer Hersteller kostet. PatientInnen, die das Medikament wollen, müssen so bis zu 200 Euro im Jahr aus eigener Tasche draufzahlen. Für einen Kostenersatz sollten nun die Patienten - insbesondere chronisch Kranke sind auf das Medikament gegen Cholesterin angewiesen - ihre medizinischen Daten der Firma gegenüber offenlegen, z.B. Rezeptbelege und Krankenkassenbescheinigungen. Sozialhilfe-EmpfängerInnen sollten sogar ihre Sozialhilfebescheide einsenden.

Erstattet werden sollen die Kosten, wenn die Lasten zwei Prozent des Bruttoeinkommen übersteigen. Bis Mitte Januar 2005 hatten schon 380 PatientInnen einen Antrag auf Erstattung bei Pfizer gestellt. Der Deutschland-Chef von Pfizer, Walter Köbele, schätzt, dass 150.000 bis 200.000 Personen sein Angebot nutzen werden. Die SPD forderte in dem Streit mit Pfizer ein Eingreifen des Datenschutzbeauftragten. Köbele versprach, dass die Daten nur für die Erstattungsaktion genutzt würden. SPD-Gesundheitsexperte Klaus Kirschner meint, Pfizer verstoße mit seinem Angebot eines Kostenausgleichs für bestimmte Patientengruppen gegen das Heilmittelwerbeverbot (Hoffmann, SZ 15./16.01.2005, 19; SZ 22./23.01.2005, 22).

Bayern

EU-Kommission geht gegen Schleierfahndung vor

Die EU-Kommission sieht in der Schleierfahndung in Bayern offensichtlich einen Verstoß gegen das EU-Recht. Dabei handelt es sich um polizeilichen Personenkontrollen in Grenznähe sowie auf Durchgangsstraßen, auch wenn kein Verdacht einer Straftat vorliegt. Aus Sicht der Kommission sind dies verdeckte Grenzkontrollen, die die Reisefreiheit einschränken. Bayerns Innenminister Günther Beckstein (CSU) hat sich mit Bundesinnenminister Otto Schily (SPD) mit der Bitte um Unterstützung in Kontakt gesetzt. Bayern rühmt sich, mit Hilfe der anlassfreien Kontrollen jedes Jahr mehrere tausend mit Haftbefehl gesuchte Personen und eingeschleuste Ausländer festzunehmen. Nach Abschaffung der Grenzkontrollen im Jahr 1995 hatte der Freistaat die Schleierfahndung eingeführt. Die EU-Kommission will offensichtlich nur jene Kontrollen verbieten, die auf die Grenzregion und Durchgangsstraßen beschränkt sind. Flächendeckend mögliche Kontrollen wie in Baden-Württemberg seien dagegen keine Grenzkontrollen durch die Hintertür und daher aus EU-Sicht erlaubt (AP 08.11.2004; SZ 09.11.2004, 36; Prantl SZ 10.11.2004, 4).

Bayern

Suizid nach DNA-Massentest

Am 26.11.2004 sprengte sich ein seit mehr als einem halben Jahr aktiver Briefbombenattentäter mit einer selbst gebastelten Bombe in die Luft. Den Suizid beging er kurz nach Beginn eines Serien-Gentests an 2300 Männern aus dem niederbayerischen Hutthurm. Der Betroffene war für den 27.11.2004 zur Abgabe einer Speichelprobe vorgeladen gewesen. Seit Anfang April hatte der 22jährige neun Briefbomben an Politiker und Behördenchefs in Bayern verschickt. Eine Sekretärin wurde bei der Zündung einer Bombe verletzt; die anderen detonierten nicht. Bei der Durchsuchung seiner Zimmers wurden Zünder und Knopfbatterien entdeckt. Die Vergleichs-DNA stammte von einem Einbruch aus einer Serie von 20 Straftaten, bei denen der Briefbomber seine genetischen Spuren hinterlassen hatte. Der Täter musste Ortskenntnisse haben, sonst hätte er die abgelegenen Häuser nicht gefunden. Daher wurde der Test auf die rund 6000 Einwohner zählende Gemeinde nahe Passau begrenzt. Ein anschließender Gentest bestätigte, dass es sich bei dem Selbstmörder um die gesuchte Person handelte. Der Massen-Test wurde daraufhin beendet (SZ 29.11.2004, 11; Kratzer SZ 27./28.11.2004, 59).

Bayern

Rigides Polizeirecht mit Telekommunikationsüberwachung

Das bayerische Kabinett hat am 23.11.2004 eine Änderung des Polizeiaufgabengesetzes (PAG) beschlossen, das u.a. die Überwachung der Telekommunikation erleichtern und ausweiten will. Im Vorjahr war ein ähnlicher Gesetzentwurf an einem breiten Widerstand inner- und außerhalb des Landtags gescheitert (vgl. DANA 2/2003, 16 f.). In einem zweiten Anlauf soll nun das Gesetz in leicht veränderter Form verabschiedet werden. Es erleichtert, so die Staatsregierung, die Bekämpfung von Terrorismus und organisiertem Verbrechen. Telefonüberwachung soll nicht erst zulässig sein, wenn die Staatsanwaltschaft wegen des Verdachtes einer Straftat ermittelt, sondern, so Innenminister Günther Beckstein, »wo die Straftaten geplant werden«. Nach dem neuen Gesetzentwurf dürfen Gespräche mit Berufsgeheimnisträgern wie Ärzten, Anwälten, Geistlichen und Journalisten nicht abgehört werden: »Der Beichtstuhl, die Arztpraxis und das Anwaltsbüro bleiben grundsätzlich tabu«. Damit trägt die Staatsregierung einem wichtigen Einwand des bisherigen Protests Rechnung. Künftig erlaubt sein soll nicht nur das Abhören, sondern auch das Unterbrechen von Telekommunikationskontakten. Netzbetreiber können gezwungen werden, die Daten von Mobilfunk-Gesprächen herauszurücken, damit die Ermittler nachträglich rekonstruieren können, wer wann mit wem und an welchem Standort telefoniert hat. An allen Grenzübergängen und auf den Autobahnen sollen Autokennzeichen automatisch registriert und mit dem Bestand des Fahndungscomputers der Polizei abgeglichen werden können. Damit, so Beckstein zur Begründung, werde auf den Kriminalitäts-Tourismus reagiert (Schneider SZ 24.11..2004, 1, 4, Bayern).

Hamburg

Senat verabschiedet neues Polizeigesetz

Am 14.12.2004 verabschiedete der Hamburger Senat die Novelle eines neuen Polizeigesetzes, die der parteilose Innensenator Udo Nagel nach einer Klausurtagung der CDU-Bürgerschaftsfraktion Ende August vorgelegt hatte. Die CDU-Fraktion hatte Druck gemacht, da eine entsprechende Gesetzesänderung seit Regierungsantritt des CDU-Schill-FDP-Senats im Oktober 2001 im Gespräch ist. Nagel übernahm im Wesentlichen den Entwurf von Schill, der nach großem Protest, u.a. von renommierten Berufsverbänden, nicht weiterverfolgt worden war.

Der Entwurf sieht langfristige Aufenthaltsverbote (bis 12 Monate), Unter-

bindungsgewahrsam (bis 14 Tage) und die Verankerung des sog. finalen Todesschusses sowie des Einsatzes von Distanz-Elektroschock-Geräten vor. Informationell sind vorgesehen: umfassende Videoüberwachung von Kriminalitätsschwerpunkten, verdachtsunabhängige Personenkontrollen, Rasterfahndung auch ohne drohende Gefahr und im Vorfeld von Straftaten, das Abhören von Telefonen und die Ortung von Handys oder »Blutproben bei Verdacht auf Infektionen zur Gefahrenabwehr«. Eine besondere Innovation sei der Einsatz von computergesteuerten Kfz-Kennzeichenlesegeräten. Die mobilen Kontrollgeräte sollen automatisch Alarm geben, wenn ein zur Fahndung ausgeschriebenes Fahrzeug vorbeifährt. Trotz leerer Staatskassen sicherte Finanzsenator Wolfgang Peiner (CDU) seinem Senatskollegen 1,5 Mio. Euro für deren Beschaffung zu.

Zurückgerudert ist Nagel im Vergleich zu Vorgängerentwürfen nur im Hinblick auf Telefonüberwachungsmaßnahmen, wo dank des Drucks von Berufsverbänden Geheimnisträger wie Ärzte, Anwälte, Journalisten und Geistliche geschützt bleiben. Nagel lobte seinen Vorschlag als »modern und effektiv«. KritikerInnen sprechen von massivem Abbau demokratischer Rechte. GAL-Bürgerschaftsabgeordnete Antje Möller klagt, Nagel habe seinen bayerischen Amtskollegen »Beckstein rechts überholt«. Weniger kritisch sieht SPD-Innenpolitiker Andreas Dressel den Gesetzentwurf: »Nagel ist übers Ziel hinausgeschossen. Die notwendige Liberalität bleibt auf der Strecke. Der Senat sollte bei diesen fundamentalen Freiheitseingriffen wieder auf den richtigen Pfad zurückkehren. Der Entwurf, der Sicherheit und Freiheit konsequent kombiniert, liegt auf dem Tisch - er kommt von der SPD.«

Kritisiert wird der Entwurf auch von Hartmut Lubomierski, Hamburgischer Datenschutzbeauftragter, und seinem Referenten Harald Wollweber. Deren Kritik richtet sich gegen die verdachtsunabhängigen Kontrollen; wo klarer formuliert werden müsse, wo und für wie lange solche Maßnahmen erlaubt sein sollen. Bei der Erlaubnis der Videoüberwachung von Kriminalitätsschwerpunkten sei nicht genügend definiert, was ein solcher Brennpunkt ist. Mit dem Begriff »wiederholte Straftaten« genügten zwei Delikte für die Installation einer Kamera. Die wiederholten Straftaten müssten »in erheblichem Umfang« begangen worden sein. Die Hauptkritik wendet sich aber gegen die »präventive Telefonüberwachung«, die sich gegen das Grundrecht auf Fernmeldegeheimnis richtet. Wollweber: »Bei Fällen der Schwerstkriminalität ist es gerechtfertigt, in das Grundrecht einzugreifen. Nach dem Senatsentwurf soll dies aber schon bei der Vorbereitung weitaus geringerer Straftaten möglich sein«, etwa bei Verdacht auf Vorbereitung einer Volksverhetzung oder einfacher Erpressung. »Wir werden anregen, dass erst bei Höchststrafen von mehr als fünf Jahren die präventive Telefonüberwachung erlaubt wird. Das ist die Grenze, die das Bundesverfassungsgericht für die Wohnraumüberwachung gesetzt hat.« Wer überwacht wurde, müsse später davon in Kenntnis gesetzt werden, um die Abhörmaßnahmen gerichtlich überprüfbar zu machen. Der Nagel-Entwurf sieht vor, dass die Unterrichtung der Belauschten dauerhaft ausgeschlossen wird. Das neue Polizeigesetz soll Sommer 2005 in Kraft treten (Gärtner, www.telepolis.de, 15.12.2004; Carini, taz nord hamburg 17.12.2004, 21; Meyer-Wellmann, www.abendblatt.de 17.12.2004 u. 05.01.2005).

Hessen

Rücknahme der Einbürgerung Dank Verfassungsschutz

Nach den Anschlägen des 11.09.2001 wurde in Deutschland die Regelanfrage bei den Ämtern für Verfassungsschutz vor einer Einbürgerungsentscheidung verbindlich vorgesehen. Im Juli 2002 hat das Regierungspräsidium Gießen einen Asylberechtigten eingebürgert, ohne aber das Ergebnis der Regelanfrage abzuwarten. Als nun die Verfassungsschützer meldeten, der Mann sei aktives Mitglied einer Tarnorganisation der kurdischen PKK, revidierte die Behörde ihre Entscheidung und nahm dem Kurzzeit-Deutschen seinen Pass wieder ab. Das Hessische Innenministerium räumte ein, dass dies nicht der einzige Fall ist, der zu einer Rückausbürgerung führte. Auch bei einem Anhänger der türkischen Islamistenorganisation Milli-Görüs hatte das Regierungspräsidium Gießen den Bericht des Verfassungsschutzes nicht abgewartet. Die Regelanfrage treibt aber auch seltsame Blüten. So verweigerte das Regierungspräsidium Darmstadt einem Türken den deutschen Pass, nachdem das Landesamt vermeldet hatte, der Wunsch-Deutsche habe vor 20 Jahren an einer Demonstration der Kommunistischen Partei der Türkei teilgenommen (Der Spiegel 2/2005, 15).

Hessen

Viele neue Befugnisse für die Polizei

Der Hessische Landtag hat am 14.12.2004 ein neues Polizeigesetz verabschiedet. Vorgesehen sind eine Vielzahl neuer Befugnisse, z.B. der »finale Rettungsschuss«. In Vordergrund stehen jedoch neue Maßnahmen der Datenerhebung. So darf die hessische Polizei im öffentlichen Verkehrsraum technische Geräte einsetzen, um Kfz-Kennzeichen elektronisch zu erkennen und mit dem Fahndungsbestand automatisiert abzugleichen, in dem gestohlene Kfz und Kennzeichen sowie Fahrzeuge, die als Tatmittel zur Begehung von Straftaten verwendet wurden (z.B. Kennzeichenmissbrauch, Urkundenfälschung, Tankbetrügerei, Einbrüche, Raubüberfälle), gespeichert sind. Mit Stand Januar 2004 gab es hessenweit 24.500 Kfz- und 44.000 Kennzeichenfahndungsausschreibungen. Wird keine Übereinstimmung mit dem Fahndungsbestand festgestellt, so soll eine sofortige automatisierte Löschung der Daten erfolgen. Zum Zweck der Eigensicherung dürfen Polizisten künftig Videoaufzeichnungen vornehmen. Begründet wird diese Maßnahme mit vergangenen Verkehrs- und Personenkontrollen mit tödlichem Ausgang. Die Telekommunikationsüberwachung wird zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erlaubt. Damit soll z.B. bei einem per Handy angekündigten Suizid der Standort des Anrufers festgestellt werden. Zugelassen wird weiterhin der Einsatz des IMSI-Catchers, über den eine Ortsbestimmung von Mobilfunkgeräten bis auf 50 Meter genau vorgenommen werden soll. Besonders »innovativ« ist die landesgesetzliche Befugnis, bei Kindern, die schwere Straftaten begehen, zusätzlich zur Erstellung von Lichtbildern und Fingerabdrücken eine erkenungsdienstliche DNA-Analyse auf Grund richterlicher Anordnung vorzunehmen (vgl. DANA 1/2004, 21 f.). In Gewahrsamszellen wird die Videoüberwachung zugelassen. Die Befugnis zur Identitätsfeststellung wird

auf Orte erweitert, an denen aufenthaltsrechtliche Verstöße von Ausländern zu vermuten sind oder an denen der Prostitution nachgegangen wird.

Der FDP-Abgeordnete Jörg-Uwe Hahn kritisierte das neue Hessische Polizeigesetz: »Die von der CDU-Alleinregierung durchgedrückten Änderungen machen deutlich, dass jedem Wunsch der Polizei kritiklos gefolgt wurde.« Es fehlten rechtsstaatliche Begrenzungen beim Kfz-Kennzeichenscanning, bei der akustischen Wohnraumüberwachung, der Telekommunikationsüberwachung und der DNA-Analyse-Anordnung: »Die FDP ist strikt gegen eine anlassunabhängige Dauerkontrolle«. Dennoch enthielt sich die FDP bei der Abstimmung. SPD und Grüne stimmten dagegen. Die Grünen kritisierten den »Gesetzgebungsaktionismus« (PE Hessisches Ministerium des Innern v. 14.12.2004; PE, www.fdp-hessen.de vom 26.11.2004; www.heise.de 15.12.2004).

Saarland

Drogen-Vortestsystem für Speichelproben

Die saarländische Polizei verfügt bundesweit als erste Polizeieinheit über ein elektronisches Drogen-Vortestsystem für Speichelproben. Das System bietet im Gegensatz zu bisher eingesetzten Vortestverfahren den Vorteil einer einfachen, schnellen und »diskreten« Untersuchung. Die Speichelprobe wird in einer Testkassette entwickelt, das Ergebnis der Auswertung und der nachgewiesene Drogentyp werden auf dem Display des Gerätes angezeigt. Mit dem System können sechs verschiedene Substanzklassen nachgewiesen werden: Cannabis, Amphetamine, Methamphetamine, Kokain, Opiate und Phencyclidin. Damit ist auch der klassische Bereich der »Designer-Drogen« erfasst (Deutsche Polizei 1/2005, 3).

Nordrhein-Westfalen/Bund

Korruptionsregister kommt

Am 15.12.2004 beschloss der Landtag in Düsseldorf für Nordrhein-Westfalen den Aufbau eines Registers der der Korruption verdächtigen Unternehmen zum Zweck des Ausschlusses bei der Vergabe öffentlicher Aufträge für eine bestimmte Zeit. Das Gesetz verpflichtet alle öffentlichen Stellen, Korruptionsfälle an das im Finanzministerium geführte Register zu melden. Dies muss bereits geschehen, »wenn kein vernünftiger Zweifel an einer schwerwiegenden Verfehlung besteht«. Kritiker des Gesetzes sehen hierin eine rechtswidrige existenzvernichtende Vorverurteilung. Bei der Vergabe von öffentlichen Aufträgen von mehr als 25.000 Euro und bei Bauprojekten von mehr als 50.000 Euro müssen die ausschreibenden Stellen beim Register nachfragen, ob der potenzielle Auftragnehmer in einen Korruptionsfall verwickelt war. Das bundesweit erste Anti-Korruptionsgesetz wird im Frühjahr 2005 in Kraft treten. Es verpflichtet u.a. auch alle Mitglieder der Landesregierung, alle kommunalen Mandatsträger sowie sachkundige Bürger in Ausschüssen, alle ihre Nebentätigkeiten anzuzeigen. Dazu zählen neben Mandaten in Aufsichtsräten und Beraterverträgen auch Funktionen in Vereinen. Bei der Innenministerkonferenz (IMK) am 19.11.2004 in Lübeck wurde die Absicht des Bundes unterstützt, die rechtlichen Grundlagen zur Errichtung eines Vergaberegisters auch auf Bundesebene zu schaffen (SZ 16.12.2004, 5; landesregierung.schleswig-holstein.de 22.11.2004).

Ausländische Datenschutznachrichten

UNO

Raffinierte Abhöranlage am UN-Sitz in Genf

Eine Sprecherin der Vereinten Nationen bestätigte am 17.12.2004 in Genf, am europäischen Sitz der Organisation sei eine »raffinierte« Abhöranlage entdeckt worden. Das gut getarnte, leistungsstarke System kam bei Renovierungsarbeiten hinter einer Täfelung im »Französischen Salon« zum Vorschein. Es soll ca. drei bis vier Jahre alt sein und aus russischen oder osteuropäischen Komponenten bestehen. Es habe bisher nicht geklärt werden können, wer für den Lauschangriff verantwortlich ist. Der »Französische Salon«, der v.a. Repräsentationszwecken dient, gehört nicht zu den wichtigsten Besprechungsräumen. Allerdings werden hier Videokonferenzen mit dem UN-Hauptquartier in New York abgehalten. Auch nutzen ihn öfters nationale Delegationen für Beratungen. Der Salon liegt neben dem Ratssaal, in dem wichtige Treffen wie etwa Abrüstungskonferenzen stattfinden (vgl. einen weiteren Abhörskandal bei der UNO DANA 2/2004, 29 f.; in der EU DANA 2/2003, 19 f.; Ulrich, SZ 18./19.12.2004, 1).

Frankreich

Mitterands Abhörskandal wird gerichtlich verhandelt

Seit dem 15.11.2004 verhandelt ein Pariser Gericht einen der großen Skandale aus der Regierungszeit des früheren Präsidenten Francois Mitterrand: Von 1983 bis 1986 hatte dieser die Telefonate von mehr als 150 FranzösInnen überwachen lassen. Die Affäre, zu der sich Mitterand nie geäußert hat, war durch die Enthüllungen der Tageszeitung Libération ruchbar geworden. Beweise für die Lauschangriffe lieferte eine unbekannt gebliebene Frau, die einem Untersuchungsrichter fünf Disketten mit etwa 5000 Gesprächs-Vermerken übergab. Seither versuchte ein Untersuchungsrichter Licht ins Dunkel dieses Vorgangs zu bringen. Ein Dutzend Angeklagte, darunter der Büroleiter der sozialistischen Premierministers, müssen sich wegen »Verletzung der Intimsphäre« verantworten. Ihre einstigen Chefs, Laurent Fabius und Pierre Mauroy, sind nur als Zeugen vorgesehen.

Ursprünglich war die Abhöreinheit des Elysée-Palastes von Mitterand als Anti-Terror-Einheit genehmigt worden. Sie war von Anfang an wenig effizient

und operierte neben den Geheimdiensten. Offenbar wurde sie vornehmlich als Instrument eingesetzt, um Mitterands Gegner auszuspionieren. So wurde z.B. ein Journalist abgehört, der gedroht hatte, die Existenz der außerehelichen Tochter des Präsidenten, Mazarine, publik zu machen. Unter Druck gesetzt verzichtete er auf eine Veröffentlichung und erreichte im Gegenzug, dass seine Steuerangelegenheiten wohlwollend gelöst wurden. Andere Journalisten, etwa von Le Monde und von dem Satire-Blatt Le Canard enchainé, wurden belauscht, weil sie Mitterand unbequem waren und zu viel wussten. Zu den Opfern gehörten neben Journalisten auch Anwälte und Geschäftsleute. Die Begründung war oft vage und lautete lakonisch »Sicherheit des Präsidenten«. Von den Beschuldigten wird ins Feld geführt, sie hätten lediglich die Anweisungen ihrer Vorgesetzten ausgeführt. Unter den Angeklagten ist kein Politiker (SZ 16.11.2004, 7).

Frankreich

Anonyme Bewerbung in Großunternehmen

Um Diskriminierungen bei der Arbeitsplatzvergabe zu bekämpfen, sollen Großunternehmen in Frankreich künftig Stellenbewerbungen anonym bewerten. Der Sozialausschuss der Pariser Nationalversammlung verabschiedete am 24.11.2004 eine Gesetzesvorlage, derzufolge Bewerbungsunterlagen in Firmen mit mehr als 250 Angestellten ohne Nennung von Namen, Geschlecht, Alter und Nationalität eingereicht und geprüft werden sollen. Sozialminister Jean-Louis Borloss relativierte die Initiative, diese werde sicher »nicht in dieser Form umgesetzt« (SZ 26.11.2004, 11).

Großbritannien

Parlament billigt Einführung einer Identitätskarte

Das britische Parlament hat mit 306 zu 93 Stimmen am 20.12.2004 ein von der Regierung eingebrachtes Gesetz zur Einführung von Personalausweisen in zweiter Lesung gebilligt. Damit scheiterte zugleich der Versuch einer fraktionsübergreifenden Gruppe von Abgeordneten der regierenden Labour-Partei und der konservativen Opposition, das Vorhaben zu verhindern. Zu Beginn der fünfstündigen Debatte verteidigte der neue Innenminister Charles Clarke den neuen Ausweis als Instrument im Kampf gegen Terror-Aktivitäten und Menschenhandel: »Die Behauptung, Personalausweise würden unsere bürgerlichen Freiheiten untergraben, ist völlig falsch. Ich glaube fest an Personalausweise.« Clarkes Rede im Unterhaus zu den Ausweisen war die erste bedeutende Amtshandlung des Nachfolgers des am 15.12.2004 zurückgetretenen David Blunkett.

Die Personalausweis-Debatte wird in Großbritannien leidenschaftlich geführt. Viele BritInnen sehen in den Ausweisen eine Beschneidung ihrer Bürgerrechte. Die Regierung erliege ihrer Obsession, alles kontrollieren zu wollen. Eine Meldebehörde, bei der man sich nach einem Umzug eintragen muss, gibt es in dem Land bisher nicht. Dennoch meldet sich die Kommune bald nach Umzügen, um von neuen Bürgern die Kommunalsteuer, die sog. Council Tax, einzufordern. Vermieter und Immobilienverkäufer sind verpflichtet, neue Bewohner zu melden. Gegner des Dokuments hatten erhofft, dass Clarke eine kritischere Grundposition zu der Karte habe und die Einführung auf die lange Bank schieben würde.

Die Gesetzesinitiative war bereits einige Wochen zuvor in der Rede der Königin angekündigt worden. Der Ausweis soll von 2008 an ausgegeben werden. Zuvor soll es eine intensive technische Testphase geben. Ab 2013 soll das Dokument Pflicht sein.

Der Kampf gegen Terrorismus und Kriminalität hatte die gesamte Thronrede der britischen Königin Elisabeth II. am 23.11.2004 geprägt. In dieser traditionell zur Parlamentseröffnung gehaltenen Rede kündigte die Königin auch ein neues Anti-Terror-Gesetz sowie die Gründung eines britischen Pendants zur amerikanischen Bundespolizei FBI an. Danach sollen in der Serious Organised Crime Agency (Soca) etwa 5000 AgentInnen tätig sein, die aus anderen Behörden abgezogen werden. Soca-Chef wird der frühere Leiter des Inlandsgeheimdienstes MI5, Stephen Lander. Von 37 Gesetzen, die die Queen für ihre Regierung ankündigte, stammen 11 aus der Abteilung »Law and Order« (Schwennicke, SZ, 22.12.2004, 5, 8; 17.12.2004, 4; 24.11.2004, 4, 6; vgl. DANA 2/2004, 29, 2/2003, 22).

USA

IT-Millionen-Flopp beim FBI

Das US-Bundeskriminalamt (Federal Bureau of Investigation - FBI) muss wegen technischer Mängel ein für den Antiterrorkampf für wichtig deklariertes Programm zur Computermodernisierung aufgeben. US-Medien berichteten, dass das FBI bereits 170 Mio. Dollar (130 Mio. Euro) in das Projekt gesteckt hat, das auf die Schaffung einer umfassenden elektronischen Datenbank abzielte. Technische und -Planungsprobleme verzögerten die Umsetzung so sehr, dass die Software inzwischen veraltet ist (SZ 15./16.01.2005, 7).

USA

Einreiseverbot für Ex-RAFlerin

Die US-Einwanderungsbehörden verweigerten dem früheren Mitglied der Roten Armee Fraktion (RAF) Astrid Proll die Ausstellung eines Visums, um ihre Mutter Hildegard Proll zu pflegen und zu beerdigen. Hildegard Proll zog 1962 in die USA, wo die Deutsche die US-Staatsbürgerschaft erwarb und US-Soldaten Deutsch unterrichtete. Ihre Tochter Astrid Proll schloss sich 1970 der RAF an. Im Mai 1972 unternahm die RAF Anschläge auf das europäische Hauptquartier der US-Armee in Heidelberg und auf das Offizierskasino des V. US-Korps in Frankfurt, weil von dort angeblich der Krieg in Vietnam organisiert wurde. Bei den Taten starben vier Menschen; 18 wurden verletzt. Astrid Proll war während der Mai-Anschläge längst verhaftet; vom Vorwurf des zweifachen Mordversuchs war sie 1971 freigesprochen worden. Die heute 57jährige Journalistin gehörte zwar der RAF an, doch hat sie weder geschossen noch Bomben geworfen. Nach ihrer Verhaftung im Frühjahr 1971 hatte sie sich vom Terror distanziert. Nach vier Jahren Haft konnte sie als ein Fall mustergültiger Resozialisierung angesehen werden. Aber nicht für die USA: Bis heute wird Proll von den USA als Sicherheitsrisiko angesehen und darf nicht einreisen. Seit Januar 2004 hat sie immer wieder vergeblich ein Visum beantragt, um ihre inzwischen 91jährige pflegebedürftige Mutter zu besuchen. Trotz einer gewissen Unterstützung

durch die US-Botschaft in Berlin wurde ihr das Visum jedes Mal verweigert. Am 05.12.2004 starb die US-Bürgerin Hildegard Proll. Sie wurde in San Francisco beerdigt. SZ-Redakteur Winkler: »Astrid Proll sitzt im kalten Berlin und fragt sich, was genau Amerikaner unter family values verstehen, was ihnen Familie bedeutet«. Der Fall Proll ist ein weiteres Beispiel für die immer restriktivere Visa-Vergabe der USA: Im Jahr 2004 bekamen schon der britische Bestsellerautor Ian McEwan und der ebenfalls aus Großbritannien stammende, zum Islam konvertierte Sänger Cat Stevens keine Einreiseerlaubnis (Winkler, SZ 11./12.12.2004, 6; Der Spiegel 51/2004, 20).

USA

Geheimes Satelliten-Spionagesystem

Trotz der Kritik aus beiden großen Parteien plant die US-Regierung weiterhin ein geheimes offenbar satellitengestütztes Spionagesystem aufzubauen. Nach einem Bericht der New York Times haben mehrere Senatoren ihre Kritik an dem Programm öffentlich gemacht, nachdem sich die Regierung weigerte, das als »verschwenderisch« bezeichnete Programm auszusetzen. Dieses wird trotz langem Widerstand bei Abgeordneten und Senatoren aus allen Lagern weiter finanziert. Die Kosten sollen von 5 auf 9,5 Mrd. Dollar angestiegen sein. Das Projekt ist das teuerste Einzelvorhaben im 40-Milliarden-Geheimdienstbudget. Der Geheimdienstausschuss des Senats hatte das erste Mal 2001 Bedenken angemeldet. Die Senatoren sind, was die Natur des Programms betrifft, zum Stillschweigen verpflichtet. Der demokratische Senator Ron Wyden nannte das Programm »unnötig, ineffizient und zu teuer«. Zahlreiche Studien hätten gezeigt, dass es für das Programm keinen Bedarf gebe. Zahlreiche andere Programme seien nützlicher, nebenbei kostengünstiger und technisch weniger riskant. John Pike von der Forschungsfirma Globalsecurity.org vermutete, dass es sich bei der Kontroverse um den Start eines Aufklärungssatelliten handele, der von der gegnerischen Abwehr nicht wahrgenommen werden kann. Diese Vermutung wurde von US-Regierungsbeamten inoffiziell bestätigt. Hintergrund der neuen Generation eines getarnten Aufklärungssatelliten soll es sein, dass Feinde ihre Militärmaterialien immer dann verlegen, wenn kein Satellit über ihr Gebiet hinwegschwebt. Kritiker bemängeln u.a., der Satellit könne nur bei Tageslicht und klarem Wetter Fotos machen (Hujer, SZ 11./12.12.2004, 8; SZ 13.12.2004, 11).

USA

Organisationsreform der Geheimdienste

Kurz vor Weihnachten 2004 hat US-Präsident George Bush mit seiner Unterschrift ein Gesetz in Kraft gesetzt, welches eine umfassende Geheimdienstreform zur Folge haben soll. Mit dem »Intelligence Reform Act« wird der weltweit größte Spionageapparat geschaffen, in den die CIA, der Abhördienst NSA mit seinem weltumspannenden Lauschkapazitäten sowie die Geheimdienste der Teilstreitkräfte, des Außen-, des Finanz- und des Energieministeriums integriert werden. 15 Dienste mit insgesamt 200.000 Angestellten und einem Jahresetat von 40 Milliarden Dollar werden unter einem Dach zusammengeführt. Damit sollen die gegenseitigen Rivalitäten und Behinderungen beendet werden, die bei der Beobachtung von Bin Laden oder allgemein bei der Bekämpfung des Terrorismus immer wieder bekannt geworden sind.

Als »Geheimdienstzar« wird ein Director of National Intelligence (DNI) über sämtliche 15 Geheimdienste bestimmen können. Als Kandidaten für den DNI-Posten sind der neue CIA-Chef Porter Goss, ein geheimdiensterfahrener Republikaner namens Thomas Kean sowie sein demokratisches Pendant Joe Lieberman gehandelt. Letzterer meinte: »Wir sind jetzt in der Lage, einen zweiten 11. September zu verhindern«. Dies bezweifeln Geheimdienstkenner, die sich nicht vorstellen können, dass die Rivalitäten zwischen den Agenten, die dem Weißen Haus unterstehen und denen, die vom Pentagon befehligt werden, aufhören werden. Der Bin-Laden-Experte und Geheimdienstkritiker Michael Scheuer meinte deshalb über den DNI: »Ihm wird der Einblick fehlen, was die einzelnen Dienste tun, und genau das ist entscheidend.« Der im Juni 2004 zurückgetretene CIA-Chef George Tenet assistierte: »Geschwindigkeit und Beweglichkeit bringen Erfolg im Krieg gegen den Terrorismus, aber nicht mehr Bürokratie.« Und einer von dessen Vorgänger, Robert Gates: »Ich fürchte, der Zar ist ein Eunuch«. Bisher sind wegen der irrationalen Regierungspolitik immer wieder aus den Diensten Indiskretionen bekannt geworden. Diese soll Bush-Freund Goss jetzt eindämmen, der für diese Aufgabe ehemalige Mitarbeiter aus dem Kongress einsetzt, die wegen ihres rüden Vorgehens mit dem Spitznamen »Hitlerjugend« tituliert werden (Mascolo, Der Spiegel 1/2005, 92 ff.).

USA

Videosystem bestellt schon mal

Die US-Firma HyperActive Technologies aus Pittsburgh testet in Fast-Food-Restaurants ihr Computersystem »HyperActive Bob«, mit dem die Bestellung von KundInnen vorhergesagt werden sollen. Ziel ist das Reduzieren von Kundenwartezeit und von überschüssig produzierten Burgern. »Bob« beobachtet mit Kameras den Parkplatz und den Eingangsbereich und erkennt, ob sich ein PKW, ein Minivan, eine Einzelperson oder eine mehrköpfige Familie nähert. Auf Basis von Erfahrungswerten zeigt ein Display den Angestellten, welche Produkte vorzubereiten sind. Eine bei McDonald´s im Einsatz befindliche Rohversion führte angeblich dazu, dass KundInnen im Schnitt eine halbe Minute kürzer auf ihr Essen warten und nur noch halb so viele überflüssige Burger produziert werden (Der Spiegel 53/2004, 119).

USA

Fotohandy als polizeiliche Ermittlungshilfe

Die Polizei von Los Angeles nutzt für die Fahndung nach flüchtigen Straftätern im täglichen Einsatz neuerdings Fotohandys oder PDA-Taschencomputer. Eingesetzt wird dabei eine radikal abgespeckte Gesichtserkennungssoftware der kalifornischen Firma Neven Vision. Der Polizist fotografiert einen Verdächtigen, dessen wesentliche Gesichtszüge elektronisch verformelt werden. Diese Daten werden mit in einer Datenbank abgelegten Fahndungsfotos abgeglichen. Die Erkennungstechnik hat der Firmengründer Hartmut Neven zusammen mit dem Bochumer Neuroinformatiker Christoph von der Mals-

burg entwickelt. Nach Ansicht von Neven ist sie nicht nur zur Verbrechersuche geeignet. Eines Tages könne etwa der Gast in fremdländischen Restaurants die Speisekarte ablichten, um sich über Internet eine übersetzte Version zu verschaffen. Oder ein Kunde fotografiert im Laden eine Ware und öffnet damit einen Link zu einer Datenbank mit Vergleichspreisen anderswo. Nevens Vision ist eine globale Bildsuchmaschine, eine Art »Google« für Bilder (Der Spiegel 4/2005, 149).

Israel

Jad Vashem veröffentlicht Holocaust-Opfer-Datenbank

Die Jerusalemer Gedenkstätte Jad Vashem hat am 22.11.2004 ihre Datenbank aller bekannten Namen von Holocaust-Opfern im Internet freigegeben. Unter www.yadvashem.org können über eine Suchmaschine die Namen von drei Millionen Namen recherchiert werden. Dies ist etwa die Hälfte der geschätzten Gesamtzahl jüdischer Opfer der Schoah. Mit der Veröffentlichung soll jeder Einzelne im Gedächtnis »wiederbelebt« werden, sagte der Direktor der Halle der Namen, Alexander Avraham. Jeder zusätzliche Name sei »ein weiterer kleiner Sieg gegen das Vergessen«.

In der Halle können Zeugen, Überlebende und andere auf Fragebögen Angaben zu ihnen bekannten Toten machen. Einer der bekanntesten Fragebögen wurde von Otto Frank ausgefüllt, der kurze Angaben über seine in Buchenwald ermordete Tochter Anne Frank machte. Die BenutzerInnen der Datenbank in englischer oder hebräischer Sprache finden kurze Angaben zur Person, darunter Geburtsort und -datum sowie Angaben - soweit bekannt - zum Todesort. Bei der Suche ist die Datenbank nicht auf die korrekte Schreibweise von Namen angewiesen. Die Suchmaschine findet auch Namen, die ähnlich klingen, aber unterschiedlich geschrieben werden.

Durch die Freigabe erhofft sich Jad Vashem weitere Informationen über ermordete Juden während des Holocaust, zumal die Zahl der Überlebenden immer mehr abnimmt. Im Internet findet sich ein Fragebogen, den ausfüllen kann, wer z.B. etwas über verschleppte oder tote jüdische Nachbarn weiß.

Finanziert durch die Auszahlung »Schlummernder Konten« auf Schweizer Banken wurden nach Angaben von Jad Vashem alle vorliegenden Namensbögen gescannt, digitalisiert und erforscht. Aus allen erdenklichen Quellen wurden Namen zusammengesucht, z.B. aus Verschickungslisten in Konzentrationslagern, Gedenkbüchern sowie Material aus dem Bundesarchiv in Koblenz (SZ 23.11.2004, 7).

Technik

Medizin bestimmt Alter auf ein Jahr genau

Für jugendliche StraftäterInnen oder AusländerInnen, die sich jünger machen wollen als sie sind, wird es schwieriger. Erstmals kombinierten Berliner Rechtsmediziner diverse Untersuchungsmethoden und können so das Alter von Heranwachsenden mit einer Genauigkeit von plus-minus einem Jahr bestimmen. Bisher betrug diese Toleranz bis zu fünf Jahren, meint Vokmar Schneider, Chef der Gerichtsmedizin an der Berliner Charité. Zwischen 50 und 70 Mal pro Jahr lassen die Berliner Ermittlungsbehörden das Alter von der Charité bestimmen. Die dortige Arbeitsgruppe zur Altersdiagnostik ist die einzige in Berlin. Im Jahr 2004 gab es mit 70 zu begutachtenden Fällen einen neuen Rekord. Chef Andreas Schmeling: »Es spricht sich herum, dass unsere Gutachten wissenschaftlich genau sind und deshalb vor Gericht Bestand haben.«

Eine solche Altersbestimmung ist v.a. bei ausländischen Jugendlichen nötig, die angeben ihre Papiere verloren zu haben. Nach deutschen Strafrecht sind Täter unter 14 Jahren nicht strafmündig. Heranwachsende bis 18 Jahren werden nach dem milderen Jugendstrafrecht belangt. Bei 18 bis 21 Jahren haben die Richter einen Ermessensspielraum, ob das Jugend- oder das Erwachsenenstrafrecht zur Anwendung kommt. Auch im Ausländerrecht hängt die Aufenthaltserlaubnis und die ausländerrechtliche Behandlung oft davon ab, ob ein Heranwachsender über oder unter 14, 16 bzw. 18 Jahre alt ist.

Es gibt verschiedene körperliche Marker für die Altersbestimmung. So entdeckte Schmelings Arbeitsgruppe, dass das Schlüsselbein nicht vor dem 21. Lebensjahr aufhört zu wachsen. Ein weiteres Merkmal sind - so Schmeling - die Weisheitszähne: »Sind diese vollständig mineralisiert, dann ist der Proband mindestens 19 bis 20 Jahre alt«. Am leichtesten ist die Bestimmung, ob ein Heranwachsender unter 14 Jahre alt ist. Unter 14 wachsen z.B. die Handknochen noch. Außerdem kann man sich am Entwicklungsstadium der weiblichen Brust oder des Schamhaares orientieren. Die Toleranz von einem Jahr ist - so Schmeling - sehr gering: »Viel genauer wird es nicht mehr.« Denn darunter beginnen individuelle Unterschiede in der körperlichen Entwicklung, die u.a. von der Ernährung und dem sozialen Umfeld abhängen (Bach, Der Tagesspiegel 23.11.2004, 9).

Sicherheitslücke bei DSL-Satellitenübermittlung

André Adelsbach und Ulrich Geveler vom Lehrstuhl für Netz- und Datensicherheit der Ruhr-Universität Bochum machten vor, wie mit minimaler Ausrüstung sensible Informationen aus der Internet-Kommunikation abgefragte werden können: Daten von Online-Shops, Kontoinformationen von KundInnen, Emails oder Kommunikationsdaten von Behörden oder privaten Firmen, wenn sie von Kunden der Satelliten-DSL-Anbieter T-Com, Netsystem oder Megasys stammen. Sie benötigten hierfür nur eine Satellitenschüssel und eine PC-Karte für den Empfang digitaler Fernsehsignale. Da die mit Satelliten-Technik übertragenen Daten im Prinzip von jedem empfangen werden können, sollten sie verschlüsselt werden. Doch verschlüsseln viele kostenlose Email-Dienste die Mails nicht, so dass sie einfach abgehört werden kön-

nen. Dies geht nur dann nicht, wenn die vom Email-Provider für das Email-Postfach angebotene SSL-Verschlüsselung genutzt wird. Von einer zweiten Sicherheitslücke waren KundInnen eines Online-Shops betroffen, auch solche, die Internet-Anschlüsse ohne Satelliten-DSL nutzten: Vom Heim-PC der KundIn bis zum Server des Shops waren die Daten korrekt verschlüsselt. Doch der Shop-Betreiber hatte diese offensichtlich via Satelliten-DSL unverschlüsselt weitergeleitet. So konnten die Bochumer vertrauliche KundInnen-Daten mitlesen (Arzt, SZ 01.12.04, 11; vgl. in diesem Heft S. 4ff).

Sichere Lügendetektion mit Kernspintomograph?

Über den Blick ins Gehirn mit Hilfe von Kernspintomographen will der amerikanische Radiologe Scott Faro präzise bestimmen können, wann ein Mensch lügt. Auf der Jahrestagung der amerikanischen Radiological Society in Chicago Anfang Dezember 2004 berichtete Faro von Experimenten, in denen er im Gehirn die Areale sichtbar machte, deren Sauerstoffgehalt des Blutes im Gewebe auf eine besondere Aktivität hinwies. Zwar könne ein Mensch beim Lügen körperliche Reaktionen bewusst unterdrücken. Aber selbst beste Pokerspieler seien nicht in der Lage, im Hirn an dem Ort, an dem die Lüge entsteht, die Nachweismöglichkeit zu verhindern. Elf Personen, von denen Faro zuvor sechs mit Spielzeugwaffen hatte um sich schießen lassen, sollten anschließend im Kernspintomographen behaupten, nicht geschossen zu haben. Während die Gehirnbilder der fünf »Unschuldigen« keine ungewöhnlichen Aktivitäten zeigten, beobachtete Faro in den Gehirnen der Täter gleichzeitige und auffällig starke Aktivitäten in Stirnhirn, Schläfenlappen und limbischem System.

Ältere Techniken messen lediglich Angst oder die Anspannung des Lügners: Im Februar 2004 präsentierte die israelische Firma Nemesyco eine Sprach-Software, die durch Lügen verursachte Frequenz-Änderungen in der Stimme entdecken soll (DANA 2/2004, 32). An der Manchester-Metropolitan-University wurde 2003 ein Kamera-Computer-System vorgestellt, das winzige Veränderungen der Mimik registriert. Und im Januar 2002 hatte der Biometrie-Forscher Ioannis Pavlidis aus Minnesota/USA einen Scanner entwickelt, der anhand von Temperaturunterschieden im Gesicht Lügen erkennen will. Mit 80%iger Treffsicherheit seien, so die Forschenden, diese Geräte genauso gut wie der weit verbreitete Polygraph, der Herzfrequenz, Blutdruck, Atemfrequenz und galvanischen Hautwiderstand misst. Diese 80% können vor US-Gerichten über schuldig oder nichtschuldig entscheiden. Entsprechend »unzuverlässig« nannte die US-amerikanische National Academy of Sciences den Polygraphen im Jahr 2003. Dennoch sind die Geräte mit dieser Trefferquote weltweit im Einsatz - z.B. bei Versicherungen, die ihre KundInnen auf Betrugshandlungen hin überprüfen wollen, oder bei der Kontrolle von MitarbeiterInnen durch Unternehmen. Im Sicherheitsbereich von Flughäfen erwarten Entwickler einen künftigen Absatzmarkt.

Auch für Hirnforscher ist dieses Gebiet eine Herausforderung. Der US-Amerikaner Lawrence Farwell hat zuletzt einen Elektroenzephalographen (EEG) zum Lügendetektor umfunktioniert: Über Elektroden am Kopf misst dieses Gerät die elektrische Spannung von Hirnströmen. Zeigt sich ein bestimmter Ausschlag der Frequenzen, sobald ein Täter mit Tatwissen konfrontiert wird, dann kann er äußerlich noch so ruhig bleiben: Die sog. P-300-Reaktion, in der 300 Millisekunden nach einer Vorhaltung im Verhör seiner Großhirnrinde an den motorischen Cortex funkt, verrät ihn. Doch selbst die EEG-Technik erwies sich nicht als täuschungssicher. Auch P-300-Reaktionen kann man üben.

Nicht verheimlichen lassen sich dagegen jene Denkvorgänge, die der Mensch als Vierjähriger erlernt. Von diesem Alter an können Kinder zwischen ihrem eigenen Wissen und dem anderer Menschen unterscheiden, wie Psychologen jüngst in Versuchen an der Universität Osnabrück nachgewiesen haben. Fortan kann das Kind Informationen gezielt für sich behalten oder etwas anderes sagen, als es denkt, um heikle Situationen zu meistern. Nach Schätzungen der Sozialforschung lügt der Mensch durchschnittlich pro Tag etwa 200 Mal mit mehr oder weniger Meisterschaft: ohne Veränderungen der Stimme, erhöhte Herzrate oder Atemfrequenz, ohne veränderten galvanischen Hautwiderstand. Mit Faros Methode meint dieser, der Möglichkeit Täter zu überführen oder Kollegen auszuhorchen, einen entscheidenden Schritt näher gekommen zu sein. Die Technik sei routinemäßig einsetzbar, prophezeien Experten wie der US-amerikanische Polygraphen-Forscher Charles Honts von der Boise State University. Sie müsse nur noch billiger werden (Wolff, SZ 07.12.2004, 10).

Billige gedruckte Polymer-RFID-Chips

Die Erlanger Firma PolyIC will Radio-Frequency-Identification-Chips (RFID-Chips) künftig mit einem einfachen Druckvorgang auf Trägerfolien produzieren. Bislang werden RFID-Chips, die kontaktlos eine Kennung an ein Lesegerät senden und künftig die heutigen Strichcodes z.B. in der Warenwirtschaft ersetzen sollen, aus Silizium hergestellt und kosten zwischen 30 und 50 Cent pro Stück. PolyIC will die Funketiketten, die ohne eigene Stromversorgung auskommen und eine integrierte Flachantenne haben, so weiterentwickeln, dass sie in der Massenproduktion nur noch einen Cent kosten. Die Firma druckt hierfür leitfähige organische Polymere als integrierte Schaltung auf dünne Folie. Vor kurzem hat sie den weltweit schnellsten organischen RFID-Chip präsentiert, der eine Taktfrequenz von 600 Kilohertz hat. Auf den Minichips mit einer geringen Höhe und mit einem Leiterbahnen-Abstand von nur 50 Mikrometern wollen die Forschenden bis 2008 96 Bit an Informationen unterbringen können. Die neuartigen Etiketten seien auch äußerst belastbar und haltbar. Selbst bei einer Temperatur von 60 Grad Celsius und einer Luftfeuchtigkeit von 100% würden die PolyIC-RFID-Chips zwei Tage lang ihren Dienst verrichten. Erste einfachere Produkte, die sich als Sicherheitsetikett an der Kasse einsetzen lassen, sollen ab 2006 eingesetzt werden. Auch der Chiphersteller Infineon arbeitet an der Plastik-RFID-Technologie. Der Traum, diese Chips massenhaft und ungeordnet lesen zu können, wird sich aber voraussichtlich nicht verwirklichen. Wolfgang Mildner von PolyIC erläutert: »Die Polymer-Technik ist zwar günstiger herzustellen, doch ist sie im Vergleich zur Silizium-Technologie in ihrer Leistungsfähigkeit begrenzt«. So funkt die jetzige RFID-Generation von PolyIC nur fünf Zentimeter weit. Viel größere Abstände, wie sie Silizium-RFIDs überbrücken, werden sich auch lang-

fristig nicht bewältigen lassen.

Analysten des Marktforschungsunternehmens In-Stat erwarten, dass sich der Umsatz mit den Funkchips von derzeit 300 Mio. Dollar in den nächsten vier Jahren verzehnfachen wird. In Deutschland will der Metro-Konzern bis Ende 2005 bereits die Lieferkette von 70% seiner Produkte vom Hersteller bis zur Ladenkasse mit RFID automatisieren und so Personal einsparen (Grote, SZ 27.01.2005, 9).

Gentechnik

Bund

Genpatente-Gesetz verabschiedet

Der Bundestag hat am 03.12.04 mit den Stimmen der Koalitionsfraktionen und der Union das lange umstrittene Gesetz über Biopatente verabschiedet. Dabei wird der Patentschutz auf menschliche Gene eng eingegrenzt. Mit dem Gesetz wird die EU-Biopatent-Richtlinie von 1998 umgesetzt. Während nach der EU-Richtlinie ein Gen oder eine Gensequenz samt der gewerblichen Anwendung patentiert werden kann, dürfen nach dem deutschen Gesetz nur Patente für eine bestimmte Funktion eines menschlichen Gens und seine Anwendung erteilt werden. Deutsches Patentrecht erlaubt damit keine Patente für Sequenzen, deren Eigenschaften noch nicht entdeckt sind. Vergeben werden dürfen Patente auf genau definierte Funktionen eines Gens und dessen medizinische Anwendung. Damit soll dem Umstand Rechnung getragen werden, dass die ca. 30.000 Gene des Menschen eine Vielzahl von Funktionen haben können.

Die Patentierung ganzer Gene war zuvor heftig wegen der damit verbundenen Einschränkung der Forschungsfreiheit und der Monopolisierung bei Pharmaprodukten kritisiert worden. Mehr als 1000 menschliche Gene sind seit 1999 nach der EU-Biopatent-Richtlinie in Europa patentiert worden. Trotz des deutschen Biopatent-Gesetzes kann das Europäische Patentamt in München weiter umfassende Patente für menschliche Gene verliehen. Sie gelten dann in ganz Europa, also auch in Deutschland.

In einem Entschließungsantrag forderten SPD und Bündnis 90/Grüne zudem die Bundesregierung auf, sich für Nachbesserungen der Richtlinie auf EU-Ebene einzusetzen. Bundesjustizministerin Brigitte Zypries (SPD), die ursprünglich einen weitergehenden Entwurf vorgelegt hatte, betonte, das menschliche Leben sei mehr als eine chemische Substanz. Die Einschränkung des Patentschutzes sei daher eine »ethisch begründete Sonderregelung«, die mit der EU-Richtlinie zu vereinbaren sei. Zuvor hatten andere Länder wie Frankreich, Italien, Spanien und Portugal die EU-Vorgabe in Frage gestellt. Durch die Eingrenzung der Patentierbarkeit erhöht sich der Druck auf Brüssel, zumindest bei menschlichen Genen die EU-Richtlinie zu novellieren. Bei dem Vorentwurf hatte die Justizministerin eine schlichte Eins-zu-Eins-Umsetzung vorgelegt. Dies wurde u.a. vom rechtspolitischen Sprecher der CDU-Fraktion, Norbert Röttgen, kritisiert. Es sei dem Parlament zu verdanken, dass der Entwurf nachgebessert wurde. Aber auch das verabschiedete Gesetz unterliegt der Kritik, da ein Patent auf Leben von Pflanzen und Tieren zugelassen wird. Die Herkunft der biologischen Substanzen, für die Patente angemeldet werden, muss künftig nicht nachgewiesen werden. Dadurch wird der genetische Ausverkauf der genetischen Ressourcen der armen Länder ermöglicht (Graupner, SZ 04./05.12.2004, 4, 5).

Deutschland

Ergebnisse vom ersten Massengentest auf Erbkrankheit

Die Ergebnisse der ersten Massengendiagnose wurden auf der Fachmesse Medica in Düsseldorf am 26.11.2004 veröffentlicht. Fast 4000 Mitglieder der Kaufmännischen Krankenkasse (KKH) hatten sich freiwillig auf die Erbanlage zur Eisenspeicherkrankheit (Hämochromatose) testen lassen. Den Mitgliedern war angeboten worden, sich auf die genetische Krankheitsveranlagung unentgeltlich testen zu lassen. Die Krankheit kann lebenswichtige Organe massiv schädigen, wenn sie nicht erkannt wird (vgl. DANA 2/2001, 45). Nach Angaben des Vorstandsvorsitzenden der KKH, Ingo Kailuweit, wurde bei 67 Menschen der Gendefekt diagnostiziert. 34 Probanden von ihnen wussten bis dahin nichts von ihrem Leiden. Bei 15 fand sich bereits zu viel Eisen im Blut; weitere 8 bedurften deshalb einer Therapie, ohne es bemerkt zu haben.

Die Resultate wurden nicht der KKH, sondern nur den Testpersonen selbst mitgeteilt. Auch die Arbeitgeber erhalten die Ergebnisse nicht. Weil die Betroffenen von ihrer Disposition wissen, können sich die Betroffenen nun regelmäßig einem Blut-Check unterwerfen, bei dem festgestellt wird, ob sich schädliche Eisenverbindungen in den Organen abzusetzen drohen. Kaluweit: »Dadurch bleibt zahlreichen Versicherten unnötiges Leid erspart, gleichzeitig können die Krankenkassen Einsparungen in Millionenhöhe erzielen«.

Nicht allen Testpersonen hilft im Fall der Eisenspeicherkrankheit ihr neues Wissen weiter. Humangenetiker Thomas Meitinger von der Technischen Universität Münster stellt fest, dass »die Mutation sich nicht zwangsläufig auswirkt«. Soweit bekannt, entwickeln nur wenige Patienten das Vollbild der Hämochromatose. KritikerInnen warnen davor, dass Menschen wegen eines Testergebnisses unnötig in Sorge gebracht werden (Berndt, SZ 30.11.2004, 10; SZ 27./28.11.2004, 6).

Deutschland

Versicherungen fürchten »Insiderwissen« der Patienten aus Gentests

Die Versicherer wollen auch über den Ablauf der Selbstverpflichtung im Jahre 2011 hinaus keine Gentests vor Abschluss eines Vertrages verlangen, erklärte Achim Regenauer, Chefarzt der Münchener Rückversicherung. Doch wenn sich Kunden von sich aus testen lassen, wollen sie die Ergebnisse auch erfahren. Der Patient solle kein »Insi-

derwissen« aus den Gentestergebnissen haben und sich damit Vorteile auf Kosten der Gemeinschaft der Versicherten verschaffen. Deshalb bestünden erhebliche Einwände gegen den Entwurf des Gendiagnostikgesetzes, das Einblicke der Versicherer in solche Gentests grundsätzlich ausschließt. (Heise, 20.01. 2005).

Kanada

Vaterschaft trotz DNA-Test ungeklärt

Zwei erwachsene Zwillinge geben einem Vormundschaftsrichter in Montreal/Kanada ein Rätsel auf: Die Frage ist, welcher der beiden Männer die inzwischen fünfjährige Tochter der gemeinsamen Geliebten gezeugt haben. Selbst der sonst übliche DNA-Vaterschaftstest bringt keine klare Antwort, da die beiden möglichen Väter ein weitgehend identisches Erbgut haben. Richter Paul Colin vom Superior Court der Proviz Quebec: »Wir sehen ein hohes Risiko, die Vaterschaft nie lösen zu können« (KielerN 13.11.2004, 60).

Großbritannien

Biologen wollen aus Y-Chromosom auf Nachnamen schließen

Ein britisches Forscherteam um David Werret vom Forensic Science Service in Birmingham arbeitet dem Magazin New Scientist zufolge daran, die für den Namen einer Person relevanten Gensequenzen des Y-Chromosoms zu identifizieren, um so z.B. über Genanalysen von Tatortspuren wie Haaren, Blut oder Sperma Täter ausfindig zu machen. Wie jedes andere Chromosom weist das Y-Chromosom familiäre Eigenheiten auf. Anders als bei den übrigen Erbgut-Paketen wird der Inhalt nicht bei jeder Zeugung mit mütterlichen Genen neu gemixt. Das Chromosom, das das männliche Geschlecht festlegt, geht unverändert vom Vater auf den Sohn über. Ausnahmen sind seltene Mutationen. Dieses männliche Beharrungsvermögen wird von Evolutionsforschenden seit einiger Zeit genutzt, um Verwandtschaftsverhältnisse in der menschlichen Ahnenreiche zu klären. Nun wollen auch Kriminalisten profitieren.

Weil Nachnamen und das Erbgut gemeinsam weitergegeben werden, ist anzunehmen, dass zwei Männer mit gleichem Y-Chromosom auch den selben Namen tragen. Ist einmal bekannt, welche Besonderheiten auf dem Y-Chromosom einer bestimmten Familie auftreten, könnte schon ein Blick ins Telefonbuch Hinweise auf den Täter liefern. Kriminalbiologe Mark Benecke meint, dass es immer wahrscheinlicher wird, dass die Namensfahndung im männlichen Erbgut tatsächlich funktioniert: »Die Datenbank mit Informationen über Y-Chromosome wächst rasch. Und die Möglichkeit, viele Merkmale parallel miteinander zu vergleichen - das so genannte Multiplexing - wird immer besser.«

Nach den derzeit geltenden Regelungen in der Strafprozessordnung dürfen Gen-Fahnder nur sog. nichtcodierende Abschnitte des Erbgutes nutzen, die nicht zu Persönlichkeitsmerkmalen gehören. Nach Ansicht von Mark Benecke gehören die für die Namenserkennung nötigen nicht zu den codierenden Gensequenzen: »Aber das ist eine politische Entscheidung«. Dem gegenüber sieht der Leiter des Instituts für Rechtsmedizin der Universität Münster, Bernd Brinkmann, »große praktische und rechtliche Probleme«: »Deutschland besitzt zwar zu Forschungszwecken die weltweit größte Datenbank für Y-Chromosomen. Sie enthält vielleicht 1000 Datensätze von Deutschen, natürlich anonymisiert. Für eine Zuordnung zu Familiennamen müssten aber hunderttausend oder mehr Datensätze samt Namen erfasst werden.« Dies rechtlich durchzusetzen sei kaum möglich und auch nicht unbedingt wünschenswert: »Ich möchte ja auch nicht, dass eines Tages die Polizei bei mir klingelt, weil irgendein Brinkmann irgendwo Spuren hinterlassen hat.«

Aus Großbritannien ist ein Fall bekannt, bei dem das Y-Namens-Chromosom zur Aufklärung eines Falles beigetragen hat: Ein Teenager hatte einen Ziegelstein von einer Brücke auf einen Lastwagen geworfen und damit den Fahrer getötet. Blutspuren des Täters passten zwar zu keinem Datensatz in dem derzeit mit 2,7 Mio. Einträgen ausgestatteten weltweit bisher umfangreichsten Genregister. Aber ein enger Verwandter des jungen Mannes war schon einmal mit dem Gesetz in Konflikt geraten. Die Ähnlichkeit der Gendaten fiel auf und brachte die Polizei auf die Spur des Täters. Rechtsmediziner Brinkmann hält es für fragwürdig, ob sich der Aufwand lohnen würde, über Jahre hinweg eine Datenbank von Y-Chromosomen aufzubauen: »Da Männer seit einigen Jahren den Namen der Ehefrau annehmen dürfen, könnte so eine Datenbank bald wieder wertlos werden.« Und auch außerehelich gezeugte Söhne und Adoptivkinder machen die Sache kompliziert. Zudem sind häufige Familiennamen oft unabhängig voneinander entstanden. Erfolg versprechender sieht es aus, wenn es nur einen Stammvater gibt und der Name seit Jahrtausenden zur Familie gehört. So konnten Analysen von Y-Chromosomen belegen, dass Männer der jüdischen Priesterfamilie Kohanom, die heute oft Namen wie Cohen, Kahn oder Kane tragen, vor 3000 Jahren tatsächlich einen gemeinsamen Ahnherren hatten. Der Überlieferung nach war es Aaron, ein Bruder Moses (Rögener, SZ 12.11.2004, 12).

Niederlande

Genproben von verurteilten Straftätern

Seit dem 01.02.2005 werden in Holland routinemäßig von bestimmten verurteilten Straftätern DNA-Proben genommen und in einer nationalen Gendatenbank gespeichert. Ziel ist es, die Aufklärungsquote von schweren Straftaten zu erhöhen. Alle Täter, die wegen Sexualstraftaten, Gewaltverbrechen oder wegen einer anderen Straftat mit einer Höchststrafe von mindestens vier Jahren verurteilt werden, müssen Speichelproben abgeben.

Gemäß den Angaben des Sprechers des Justizministeriums, Ivo Hommes, konnten bisher nur DNA-Proben genommen werden, wenn dies im Interesse von laufenden Ermittlungen lag. Jetzt würden auch bereits Verurteilte in den Genabgleich mit einbezogen. Die Verformelung der Proben wird in einer Datenbank gespeichert und mit den Analyseergebnissen von Genspuren verglichen, die an Tatorten gefunden wurden.

Derzeit sind in der nationalen Datenbank die DNA-Profile von 6000 namentlich bekannten Menschen gespeichert. Mit dem neuen Gesetz soll die Zahl auf etwa 9000 erhöht werden. Zusätzlich verfügen die niederländischen Behörden über 12.000 Proben von Unbekannten, die an Tatorten sichergestellt wurden (SZ 02.02.2005, 7).

Rechtsprechung

Lordrichter des britischen Oberhauses

Anti-Terror-Gesetze verfassungswidrig

Das höchste britische Gericht hat am 16.12.2004 die Anti-Terror-Gesetze der Regierung Blair als schwere Verletzung der Menschenrechte verurteilt. Die Gesetze seien mit rechtsstaatlichen Grundsätzen unvereinbar und verstießen gegen die Europäische Menschenrechtskonvention. Neun muslime Ausländer, die als Terroristen verdächtigt und seit über drei Jahren ohne Prozess in Gefängnissen festgehalten werden, hatten Klage vor den Lordrichtern des britischen Oberhauses, dem höchsten britischen Berufungsgericht sowohl in Straf- als auch in Zivilsachen, erhoben. Da es in Großbritannien kein Gericht gibt, das über dem Parlament steht, müssen nun die Abgeordneten entscheiden, ob die Inhaftierten freigelassen werden. Ein Sprecher des Innenministeriums sagte, zunächst blieben die Betroffenen in Haft. Ihre Anwälte hatten mitgeteilt, einige der Gefangenen litten an psychischen Problemen, da sie noch nicht einmal den Grund ihrer Inhaftierung wüssten. Die Anti-Terror-Gesetze waren kurz nach den Anschlägen vom 11.09.2001 im Schnellverfahren verabschiedet worden. Sie erlauben es u.a., Ausländer auch ohne Anklage und Prozess auf unbestimmte Zeit festzuhalten, wenn der Innenminister den »begründeten Glauben« hat, dass der Betreffende eine Gefahr für die nationale Sicherheit darstellt. Auf dieser Grundlage waren mittlerweile 600 Menschen festgesetzt worden.

Lord Nicholls of Birkenhead: »Unbegrenzte Inhaftierung ohne Anklage oder Prozess ist jedem Rechtsstaat ein Gräuel. Das bringt die inhaftierte Person um jeden Schutz, den ein Strafprozess bieten soll.« Lordrichter Leonard Hoffmann: »Die wahre Bedrohung für das Leben der Nation geht nicht vom Terrorismus aus, sondern von Gesetzen wie diesem.« Damit erwies sich einmal mehr die Justiz als Garant für Rechtsstaatlichkeit und Vernunft im Zeitalter der Terrorhysterie. November 2004 hatte ein US-Bundesrichter den Präsidenten George Bush daran erinnert, dass er trotz aller Macht »kein Gericht« sei. Und der deutsche Bundesgerichtshof hat im Fall des Verdächtigen Mounir el-Motassadeq erklärt, der Terrorkampf dürfe »kein wilder ungeregelter Krieg« sein (Richter, SZ 20.12.2004, 4, SZ 17.12.2004, 7).

EuGH

Telekom darf an Teilnehmerdaten nichts verdienen

Der Europäische Gerichtshof (EuGH) in Luxemburg hat in einem niederländischen Streit entschieden, dass sog. Universaldienstanbieter wie z.B. die Deutsche Telekom an der Weitergabe der zentralen Teilnehmerdaten nichts verdienen dürfen. Zu den »Basisdaten« gehören danach Name, Anschrift und Telefonnummer. Die Weitergabe weiterer Daten, z.B. zu Beruf, oder interner Kundendaten wäre dagegen wegen einer Verletzung der Privatsphäre der Teilnehmer unzulässig (Rs: C-109/03). Die Telekom wollte das Urteil zunächst nicht bewerten. Die Praxis in Deutschland ist von den Vorgaben des EuGH aber offenbar gedeckt. Ein Konkurrent des niederländischen Telefonkonzerns KNP will die Telefondaten des Landes auf CD-ROM und im Internet anbieten. Der EuGH entschied, die KPN müsse hierfür die »Basisdaten« herausgeben, soweit die Kunden ihren Eintrag in Telefonbücher nicht abgelehnt haben. Die Weitergabe anderer Daten können nach dem Luxemburger Urteil nach nationalem Recht zugelassen werden (SZ 26.11.2004, 11).

BVerwG

Ex-Milli-Görüs-Mitglied kein Sicherheitsrisiko

Gemäß einem Urteil des Bundesverwaltungsgerichtes (BVerwG) in Leipzig vom 10.11.2004 (Az. 3 C 33.03) reicht die Mitgliedschaft in der islamistischen Gemeinschaft Milli Görüs allein nicht aus, einem Flughafenangestellten die luftverkehrsrechtliche Zuverlässigkeit abzusprechen und ihm den Zutritt zu Sicherheitsbereichen zu verweigern. Der 1974 in Deutschland geborene, hier zum Handwerker ausgebildete und im August 2001 eingebürgerte Mann arbeitete seit 2000 im Ladedienst des Münchner Flughafens. Er ist verheiratet und hat zwei Kinder. Bei einer erneuten Zuverlässigkeitsprüfung aus Anlass der Terroraktionen vom 11.09.2001 teilte das Bayerische Landesamt für Verfassungsschutz der Luftfahrtbehörde mit, dass der Betreffende von 1996 bis 1998 Mitglied und Ansprechpartner für die Jugendlichen bei einem Ortsverein von Milli Görüs gewesen sei. Darauf hin entzog ihm das Luftamt die Zutrittsberechtigung. Klage und Berufung des Mannes dagegen blieben zunächst ohne Erfolg. Der Bayerische Verwaltungsgerichtshof (VGH) hatte sein Urteil darauf gestützt, dass Milli Görüs langfristig das Ziel verfolge, Staat und Gesellschaft in Deutschland und Europa zu islamisieren und die Gleichberechtigung von Mann und Frau sowie die Religionsfreiheit außer Geltung zu setzen. Die Mitgliedschaft und aktive Betätigung in einer solchen verfassungsfeindlichen Gemeinschaft begründe die Vermutung mangelnder Zuverlässigkeit.

Der 3. Senat des BVerwG gab dagegen der Revision des Klägers statt und hob den angefochtenen Bescheid auf. Zwar müsse die Feststellung des VGH zu Grunde gelegt werden, dass Milli Görüs verfassungsfeindliche Ziele verfolge - dies erklärtermaßen aber ohne Gewalt. Die Ausrichtung des Vereins biete daher kein Indiz für eine Gewaltbereitschaft eines einzelnen Mitglieds. Vielmehr sei im Einzelfall festzustellen, ob ein Verstoß gegen die Sicherheit des Luftverkehrs zu befürchten sei. Dabei müssten zwar strenge Maßstäbe angelegt werden. Der Kläger sei jedoch nur kurz Mitglied bei dem Verein gewesen und inzwischen in hohem Maße in die deutsche Gesellschaft integriert. Weitere Anhaltspunkte, dass er die Sicherheit des Luftverkehrs gefährden könne, seien aber nicht bekannt geworden (Mül-

ler-Jentsch, SZ 12.11.2004, 1, 4, Lokales).

VG Köln

Scientology bleibt unter Beobachtung

Das Verwaltungsgericht Köln (VG) wies am 11.11.2004 ein Klage von Scientology gegen die Bundesrepublik zurück, mit der deren Observierung durch das Bundesamt für Verfassungsschutz gerichtlich gestoppt werden sollte (Az. 20 K 1882/03). Zur Begründung erklärte das Gericht, es lägen »tatsächliche Anhaltspunkte« für Bestrebungen der Scientologen vor, die gegen die freiheitlich-demokratische Grundordnung gerichtet seien.

Das VG Köln wies in seiner Begründung auf eine Vielzahl teilweise nicht öffentlich zugänglicher Quellen hin, wonach die Organisation wesentliche Grund- und Menschenrechte außer Kraft setzen oder einschränken wolle. Als Beispiel nannte das Gericht die Menschenwürde, das Recht auf freie Entfaltung der Persönlichkeit und das Recht auf Gleichbehandlung. Scientology strebe eine Gesellschaft ohne allgemeine und gleiche Wahlen an. Diese »verfassungsfeindlichen Zielsetzungen« rechtfertigten die weitere Beobachtung durch den Inlandsgeheimdienst. Dem stehe nicht entgegen, dass sich Scientology als Kirche bzw. Religionsgemeinschaft verstehe. Die Beobachtung von Scientology durch die Verfassungsschutzämter geht auf einen Beschluss der Innenministerkonferenz von 1997 zurück. Im Verfassungsschutzbericht für das Jahr 2003 wird der Organisation vorgehalten, weiterhin in »verfassungsfeindlicher Zielsetzung auf die Willensbildung ihrer Mitglieder« einzuwirken. Unter anderem werde Funktionsträgern und Mitgliedern in Kursen »antidemokratisches Denken und Handeln« vermittelt (SZ 12.11.2004, 8).

OLG Karlsruhe

Mail-Filterung ist strafbar

Gemäß einem Urteil des Oberlandesgerichts Karlsruhe ist das gezielte Ausfiltern der Email eines bestimmten Absenders strafbar, wenn kein besonderer Rechtfertigungsgrund vorliegt. Im konkreten Fall hatte eine Hochschule veranlasst, dass alle von einem Ex-Mitarbeiter stammenden und an ihn gerichteten Emails ausgefiltert werden, ohne dass hierüber Absender und Empfänger unterrichtet wurden. Dies wurde als eine Verletzung des Post- und Briefgeheimnisses geahndet (SZ 18.01.2005, 6).

OLG Koblenz

Eheleute sind untereinander auskunftspflichtig

Das Oberlandesgericht (OLG) Koblenz hat entscheiden, dass eine geschiedene Ehefrau Anspruch auf Auskunft über das eheliche Vermögen hat. Nur so sei es ihr möglich, eventuelle Zahlungsansprüche im Zusammenhang mit dem sog. Zugewinnausgleich zu prüfen. Das OLG hob damit eine Entscheidung des Amtsgerichts Alzey auf und gab der Auskunftsklage der Frau statt. Diese hatte zuvor ihren Ex-Ehegatten vergeblich aufgefordert, ihr Auskunft über den Stand des ehelichen Vermögens zum Zeitpunkt der Scheidung zu geben (Az. 11 UF 742/03; SZ 21.01.2005, 6).

BSG

Anspruch auf Patientenquittung

In einem am 08.12.2004 verkündeten Urteil bekräftigte das Bundessozialgericht (BSG) in Kassel den Anspruch gesetzlich versicherter Patienten auf die sog. Patientenquittung (Az. B 1 KR 38/02 R). Ärzte können sich nicht darauf zurückziehen, dass die Kassenärztliche Bundesvereinigung (KBV) die hierfür vorgesehenen Ausführungen noch nicht beschlossen hat. Gemäß dem Urteil waren Ärzte schon nach der Ende 2003 ausgelaufenen Vorgängerregelung »zumindest auf entsprechendes Verlangen« verpflichtet, ihren Patienten Auskunft über die von ihnen abgerechneten Leistungen zu geben.

Seit Jahresbeginn 2004 können gesetzlich Versicherte von ihrem Arzt Auskunft verlangen, welche Leistungen er mit ihrer Kasse abgerechnet hat und wie hoch hierfür das ungefähre Honorar sein wird. Zuvor hatte das Sozialgesetzbuch V dem Wortlaut nach sogar eine automatische Auskunft vorgesehen, die aber nicht beachtet worden ist, weil KBV und Krankenkassen die laut Gesetz vorgesehene Detailregelungen nicht erlassen haben. Beide hatten den Verwaltungsaufwand als »Ressourcenverschwendung« abgelehnt. Das BSG stellte nun aber fest, dass der Gesetzgeber den Auskunftsanspruch der Patienten nicht von einer Vereinbarung der Spitzenverbände der gesetzlichen Krankenversicherung abhängig machen wollte. Wegen der Vergleichbarkeit der gesetzlichen Neuregelung dürfte diese Aussage auch für die jetzige Patientenquittung gelten (SZ 09.12.2004, 6; vgl. auch S. 20).

LG Bonn

Nachbar darf auch keine Videokamera-Attrappen aufstellen

Ein Hauseigentümer hatte im Dachfenster Videokameras aufgestellt, mit denen er Teile seines Grundstücks, aber auch das des Nachbarn überwachen konnte, nachdem es wiederholt zu Beschädigungen an Haus, Garage und PKW gekommen war. Der Nachbar klagte auf Beseitigung, da er sich in seinen Persönlichkeitsrechten beeinträchtigt sah. Das Landgericht Bonn gab ihm in seiner Entscheidung vom 16.11.2004 (Az. 8 S 139/04) Recht.

Zwar hatte der Beklagte vorgetragen, mittlerweile nur noch Attrappen aufgestellt zu haben, dies hielt das Gericht aber nicht für wesentlich. Da für die Betroffenen tatsächlich nicht erkennbar war, ob sie nun gefilmt wurden oder nicht, müssten sie ständig mit einer ihren Privatbereich überwachenden Aufzeichnung rechnen. Dieser Überwachungsdruck sei ein so gewichtiger Eingriff in das Persönlichkeitsrecht, der auch unter Berücksichtigung der rechtlich geschützen Belange des Beklagten nicht gerechtfertigt sei.

Die Art und Weise der Videüberwachung sei auch weder geeignet noch verhältnismäßig. Damit könne nur ein kleiner Teil des Grundstücks überwacht werden, der von Sachbeschädigungen betroffen gewesen sei. Außerdem könne die Videoüberwachung nach Aussage des Sachverständigen auch in anderer Weise vorgenommen werden, indem die Kameras nicht im Dachfenster, sondern außerhalb des Gebäudes an einem Schuppen oder einer Mauer angebracht werden, und damit den Kläger nicht beeinträchtige. *(rs)*

Buchbesprechungen



Simitis, Spiros

Der verkürzte Datenschutz - Versuch einer Korrektur der Defizite und Diskrepanzen im justitiellen und Sicherheitsbereich der Europäischen Union

Nomos Verlagsgesellschaft Baden-Baden, 2004, 83 S., ISBN 3-8329-0878-1

(tw) Das kleine Büchlein beruht auf einem für das Bundesministerium der Justiz erstatteten Gutachten. Simitis analysiert darin die Rahmenbedingungen - genauer die Schwachstellen - des Datenschutzes bei den innen- und rechtspolitischen Aktivitäten der Europäischen Union. Es geht also um die personenbezogene Datenverarbeitung bei Schengen, Europol, Eurodac, Eurojust, bei den Übereinkommen über den IT-Einsatz und die Zusammenarbeit der Zollverwaltungen und das Übereinkommen über die Rechtshilfe in Strafsachen zwischen den EU-Mitgliedstaaten. Dabei kommt Simitis - mit der für ihn bezeichnenden und prägnanten Sprache - zu dem Ergebnis, dass es keinen kohärenten Datenschutz in diesem sich eher chaotisch entwickelnden Rechtsbereich gibt. Die Bezugnahmen auf die Rechtsgrundlagen, die Regelungen zu Zweckbindung und Datenübermittlung oder die Datenschutzkontrolle sind derart unübersichtlich, dass weder Experten, geschweige denn die Betroffenen wissen können, woran sie sind. Statt sich auf die moderne Grundrechte-Charta und die EU-Datenschutzrichtlinie zu beziehen, wird teilweise noch auf die überholte Datenschutzkonvention des Europarates Bezug genommen. Bei den Betroffenenrechten gibt es teilweise Meistbegünstigungsklauseln, aber teilweise auch rigorose Beschränkungen, bei der Datenschutzkontrolle ist teilweise der Europäische Datenschutzbeauftragte, teilweise sind (unterschiedliche) gemeinsame Kontrollinstanzen, teilweise sind die nationalen Datenschutzaufsichtsbehörden zuständig ...

Dieser Zustand hat, dies analysiert Simitis richtig, politische Ursachen: Während bei der Schaffung neuer Instrumente zur Straftatbekämpfung und für die sog. Innere Sicherheit oft innerhalb kürzester Zeit Konsens gefunden wird und Maßnahmen rigoros umgesetzt werden, besteht bei den politisch Verantwortlichen scheinbar kein Handlungsdruck, wenn es um den Datenschutz geht, obwohl von Seiten der Datenschutzkontrollinstanzen dauernd Vereinheitlichungen auf hohem Niveau eingefordert wurden und werden. Lediglich das insofern weitgehend machtlose Europäische Parlament macht teilweise eine Ausnahme.

Simitis versucht in einem letzten Kapitel über 17 Grundsätze einheitliche Prinzipien zu entwickeln, an denen sich der Datenschutz der europäischen Innen- und Justizpolitik orientieren könnte bzw. sollte. Diese Grundsätze sind umfassend und voll zu unterstützen. Doch gerade in diesen Thesen liegt die einzige Schwäche des ansonsten brillanten Gutachtens: Die Grundsätze bleiben zu allgemein, als dass direkte Regelungsansätze abgeleitet werden könnten, die insbesondere die Informationsbeziehungen zwischen den bisher nebeneinander bestehenden europäischen und nationalen Instrumenten berücksichtigen. Wie können - jenseits des Allerweltszwecks »Sicherheit« spezielle Zwecke definiert werden und in Form von Informationsbeziehungen zugelassen und ausgeschlossen werden? Simitis liefert aber auch Ansätze, die für die nationalen Diskussionen innovativ sind, etwa wenn er fordert, dass in dem Bereich der inneren Sicherheit mit seiner höchst individualisierten Datenverarbeitung der pseudonymen Verarbeitung grundsätzlich der Vorrang gegeben werden müsse. Auch wenn der Autor nicht mehr in der vordersten Linie der aktuellen Datenschutzdiskussion steht, so ist sein Büchlein eine wichtige Bereicherung für die Datenschutzdiskussion in einem ansonsten eher unterbelichteten Segment des Datenschutzes.



Beckhusen, G. Michael

Der Datenumgang innerhalb des Kredtinformationssystems der SCHUFA

Nomos Verlag Baden-Baden 2004,
359 S., ISBN 3-8329-0994-X

(tw) Doktorarbeiten zum Datenschutz gibt es inzwischen viele. Doch bei vielen ist der Erkenntniswert nicht allzu hoch, wird doch das, was inzwischen zu einem Thema veröffentlicht wurde, zumeist nur neu zusammengefasst und zum x-ten Mal kommentiert. Insofern in mancher Hinsicht eine erfreuliche Ausnahme ist das Buch von Beckhusen zur Schufa, das von der Forschungsstelle für Datenschutz an der Johann-Wolfgang-Goethe-Universität unter der Rubrik »Frankfurter Studien zum Datenschutz« herausgegeben wird. Erfreulich zunächst die schnelle Produktionszeit: Die in Bremen abgelieferte Dissertation berücksichtigt die Literatur bis Juli 2004 und war schon Ende 2004 gedruckt verfügbar. Verarbeitet ist weitgehend die veröffentlichte Literatur zur Schufa. Aber nicht nur das. Durch weitere Recherchen ist die Arbeit auch faktisch auf der Höhe der Zeit, wenn die Ausweitungen der Geschäftsfelder der Schufa, z.B. in den Be-

reich der Wohnungswirtschaft, behandelt werden oder aktuelle Angebote wie z.B. die Evidenzzentrale für abhanden gekommene Ausweispapiere (EVA), das Decision Support System (DSS) und natürlich der Auskunft-Scoring-Service ASS. Die verschiedenen Verfahren werden präzise faktisch beschrieben und dann einer rechtlichen Würdigung unterzogen.

Dabei vertritt der Autor abgewogene und begründete Positionen, die trotz der teilweise komplexen rechtlichen und tatsächlichen Zusammenhänge gut verständlich präsentiert werden. Die Ergebnisse sind für die Schufa nicht nur schmeichelhaft. So relativiert der Autor zu Recht die von der Schufa immer wieder herausgestellte verbraucherschützende Wirkung des Systems. Die praktizierte Auskunftserteilung z.B. bei bestrittenen Forderungen wird kritisch kommentiert, bestimmte Angebote, z.B. die Übermittlung der Merkmals Energiemissbrauch wird als rechtswidrig verworfen. Es wird festgestellt, dass einige AGB-Klauseln der Schufa rechtswidrig sind. Auf Fehlerquellen im Verfahren durch ungenügende Prüfung von Anfragen wird hingewiesen. Bei einigen Aspekten vertritt Beckhusen Positionen, die aus juristischer Sicht zwar begründbar sind, aber den praktischen Datenschutzanforderungen nicht genügen, etwa, wenn er meint, eine Bagatellgrenze sei rechtlich nicht geboten, wenn er den Widerruf einer Einwilligung zur Datenverarbeitung über die rechtliche Konstruktion des »venire contra factum proprium« einschränken will, wenn er bei der Frage bereichsübergreifender Datennutzungen keine klaren Grenzen definiert, wenn die Gebührenerhebung aus verfassungsrechtlicher Sicht nicht weiter problematisiert wird. Nicht überzeugend, aber im Ergebnis ohne wesentliche Auswirkungen sind auch seine Ausführungen zum »Bankgeheimnis«. Äußerst erfreulich ist die intensive Auseinandersetzung mit dem Scoring. Hierbei setzt der Autor einen klaren Kontrapunkt zu einigen - leider immer noch nicht überholten - Positionen, die das Scoring teilweise aus dem Datenschutzrecht völlig herausnehmen wollen. So wird z.B. im Ergebnis dem Betroffenen ein Anspruch auf die Auskunft des Scorewertes zugestanden.

Nützlich sind ein ergiebiges Literaturverzeichnis und relevante Fußnoten, eine konsistente Zusammenfassung der Ergebnisse sowie eine Gliederung, die das Auffinden von Fragestellungen auch dann ermöglicht, wenn man das doch sehr umfangreiche Buch nicht von Anfang bis Ende durchlesen kann und will. Das Buch gehört auf den Schreibtisch jedes Schufa-Justiziars und -Datenschutzbeauftragten, jedes mit Kreditvergabe beschäftigten Banken-Justiziars, jedes für den Datenschutz zuständigen Mitarbeiters von Verbraucherzentralen und Aufsichtsbehörden. Vielleicht kann es dazu beitragen, dass die jüngst immer mehr außer Kontrolle geratende Schufa wieder zurück auf den Boden des Rechts geholt werden kann.



Sélitrenny, Rita

Doppelte Überwachung - Geheimdienstliche Ermittlungsmethoden in den DDR-Untersuchungsanstalten

Christoph Links Verlag Berlin, Oktober 2003, 517 S., ISBN 3-86153-311-1

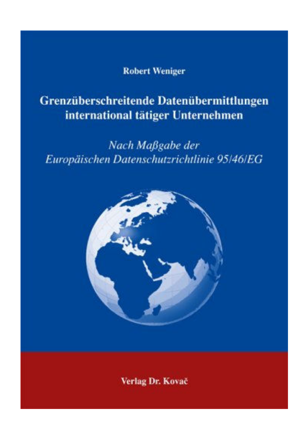
(tw) Die breite öffentliche Beschäftigung mit dem Nazi-Strafjustizsystem begann erst 20 Jahre nach Beendigung des nationalsozialistischen Terrors. Es ist zu hoffen, dass die Entdeckung des DDR-Strafsystems in der öffentlichen Diskussion und insbesondere im Rahmen der wissenschaftlichen Aufarbeitung früher erfolgt. Während vielen Teilen des Ministeriums für Staatssicherheit (Stasi) sofort nach der Wende ausreichende Aufmerksamkeit zuteil wurde, kann dies bisher für das Untersuchungshaft- und Strafvollzugssystem nicht behauptet werden. Mit der Veröffentlichung der Doktorarbeit der aus der DDR-Bürgerrechtsbewegung stammenden Rita Sélitrenny liegt nun ein Grundlagenwerk vor, das Ausgangspunkt für weitere Forschungen und für Debatten sein kann.

Zur Nazistrafjustiz besteht inzwischen die nötige zeitliche und persönliche Distanz, um sich mit deren offensichtlicher Willkür ausreichend objektiv auseinandersetzen zu können. Ganz so einfach ist es mit dem DDR-System nicht. Dies ist Grund genug, sich vor allem als Wessi- aber auch als Ossi-Jurist dem Thema zu nähern. Das DDR-Straf(un)recht ist nicht nur zeitlich wenig weit entfernt, es ist im Rahmen der juristischen Aufarbeitung schon zum Bestandteil des neuen gesamtdeutschen Rechts geworden. Die Betroffenen auf beiden Seiten sind nach der Wende aktiv. Für die gesellschaftliche Rehabilitation der Justizopfer fehlt es oft am Verständnis für das DDR-Strafsystem. Hierin gibt die Autorin unter akribischer Auswertung von Stasi-Unterlagen, Dienstvorschriften, juristischen DDR-Doktorarbeiten, sonstigen DDR-Unterlagen, von Literatur und Betroffenenberichten tiefe Einblicke.

Ausgehend von dem Begriff des »Doppelstaates« von Ernst Fraenkel ordnet sie das DDR-Straf- und -Gefängnissystem in die Kategorien »Normenstaat« und »Maßnahmestaat« ein und entwickelt als Beschreibung den treffenden Begriff des »Normensimulationsstaates«, der an der ideologischen Front zu den westlichen Demokratien unter besonderer Beobachtung stand. Materialreich beschreibt die Autorin das politische Strafrecht, das Strafprozessrecht, die Einbindung der Polizei, des dominierenden Staatssicherheitsapparates und des Justizapparates mit den Staatsanwaltschaften in die strafrechtlichen und strafvollzuglichen Strukturen. Dabei ist die Faktendarstellung in einzelnen Kapiteln ermüdend, wenn historische Abläufe, Organigramme, Dienstvorschriften und Bewertungen von maßgeblichen Funktionären referiert werden. Aber gerade diese Lektüre vermittelt wohl ein authentischeres Bild des DDR-Strafsystems als manch ideologisch geprägte Darstellung aus Ost- oder Westsicht. Sie gibt Einblicke in Hintergründe, wie sie auch Betroffenenberichte nicht bieten können. Äußerst aufschlussreich sind die Einzelfallbeispiele, die beschreiben, wie sich das System - bar jeder menschlichen Erwägung - der Schwächen der Menschen bediente, wie aber doch der Mensch als solcher dennoch oft überleben konnte.

Hinter einer formellen äußeren Fassade verbarg sich ein ausgeklügeltes intransparentes informelles System des Zusammenwirkens, das darauf abzielte, die Gesellschaft und die Menschen darin unter Kontrolle zu halten und hierfür auch das Strafsystem zu nutzen.

Wichtiger als die Sanktion war für diesen DDR-Apparat die Information, die er sich u.a. auch durch Zelleninformatoren, durch die Einbindung von Gefangenen in die Informationsstrukturen von Justiz, Polizei, Staatssicherheit und Partei beschaffte. Insofern ist das Buch ein Lehrstück über den Einsatz von Menschen, die im neuen gesamtdeutschen Kontext V-Leute genannt werden. Es ist ein Lehrstück für den Missbrauch des Strafrechts für politische Zwecke und ein Lehrstück über die Wirkung der Aufhebung informationeller Trennungen, wie sie derzeit in Deutschland im Rahmen der Diskussion um die Terrorismusbekämpfung verstärkt gefordert wird. Von dokumentarischem Wert sind die Namens-, Kader- und Literaturverzeichnisse.



Weniger, Robert

Grenzüberschreitende Datenübermittlungen international tätiger Unternehmen - nach Maßgabe der Europäischen Datenschutzrichtlinie 95/46/EG

Verlag Dr. Kovac Hamburg, 2005,
600 S., ISBN 3-8300-1779-0

(tw) Der Datenexport - der internationale Datenverkehr - ist aus Datenschutzsicht ein Thema, das derzeit nicht im Zentrum der Datenschutzdiskussion steht, das es aber doch immer wieder bis zu Schlagzeilen auf Titelseiten bringt, etwa wenn die USA Fluggastdaten von internationalen Fluglinien einfordern oder wenn es um den Datenaustausch zur Bekämpfung des internationalen Terrorismus geht. Auch wenn der Titel diesen Eindruck nicht vermittelt - die Rede ist ja nur von »international tätigen Unternehmen« - so finden wir in dem dicken Buch von Weniger hierzu ebenso wertvolle Informationen wie zu »safe harbour«, Standardvertragsklauseln oder »codes of conduct« beim internationalen Datenaustausch in und durch Unternehmen. Aber nicht nur das: Die Doktorarbeit lässt eigentlich kaum ein Datenschutzthema aus: Sie beschreibt die Geschichte der Telekommunikation ebenso wie die Geschichte der Datenschutzgesetzgebung, die datenschutzrechtliche Terminologie ebenso wie Spezialthemen vom Umgang mit genetischen Erbinformationen über Videoüberwachung bis hin zur Kryptographie, vom Datenschutz durch Technikgestaltung bis hin zum marktwirtschaftlichen Datenschutz. Dabei zeigt schon das Literaturverzeichnis die Belesenheit des Autors, der nicht nur junge Veröffentlichungen zitiert, sondern auch alte Klassiker in Erinnerung bringt. Trotz vieler Umwege kommt der Autor dann doch auf die wichtigen Fragen des internationalen Datenaustauschs zu sprechen und beschreibt in gut verständlicher Sprache die wichtigsten Aspekte, Probleme und Lösungsansätze.

Das Buch gibt einen guten Überblick wirklich fast über sämtliche in der Datenschutzdiskussion derzeit angesprochenen Fragen. Dabei verbleibt der Autor weitgehend auf der deskriptiven Ebene, was angesichts der Vielzahl der angesprochenen Themen auch kein Wunder ist. Dort wo er Position bezieht, ist dies eine fortschrittliche, d.h. sie ist grundrechts- und marktorientiert. Woran es der Arbeit fehlt, ist Originalität. Das Problem vieler juristischer Doktorarbeiten liegt darin, dass sie ausführlich Literatur auswerten, Probleme beschreiben und deren Lösungsdiskussion referieren. Oft kommt dabei die persönliche Note der Autoren zu kurz. Dies gilt auch für Wenigers Arbeit. Dies äußert sich u.a. darin, dass keine - wie bei Promotionen üblich - abschließende Thesen referiert werden. Interessant an dem Buch ist Folgendes: Der Wechsel von der klassischen Bibliotheksrecherche hin zur Recherche im Internet: Der Autor orientiert sich über weite Strecken an Texten, die auch oder sogar ausschließlich im WWW dokumentiert sind. Manch grundlegender Aufsatz aus der Papierwelt wird nicht zitiert, wohl aber manche elektronische Quelle, die sonst wenig wahrgenommen wird. Das für Doktorarbeiten typische Fehlen eines Stichwortverzeichnisses wird weitgehend kompensiert durch ein klares und aussagekräftiges Inhaltsverzeichnis. Das Buch ist dadurch eine gute Nachschlagequelle für viele Fragestellungen zum Datenschutz, nicht nur aber auch, soweit es um grenzüberschreitende Übermittlungen geht.

Zitate

Jacques Rogge, Präsident des Internationalen Olympischen Komitees über unangekündigte Dopingkontrollen bei LeistungssportlerInnen auf die Frage: »Also Big Brother im Sport, die totale Überwachung des Athleten?«:

»Ja, Betrüger zerstören die Glaubwürdigkeit. Und wir haben Big Brother überall in der Drogenbekämpfung. Also ich habe kein Problem damit, es geht ja um Betrugsbestrafung. Wenn da jemand sein Recht auf Privatsphäre einklagen will - ich bitte Sie.«

Salma Hayek, Schauspielerin, findet E-Mails fürchterlich:

»Ich bekomme überhaupt nichts von dieser Person, die mir da schreibt - keine Handschrift, keinen Kaffeefleck auf dem Papier, keinen Tintengeruch. E-Mails sehen alle gleich aus. Egal, ob ich eine E-Mail von jemandem bekomme, den ich liebe oder von jemandem, den ich hasse. Jegliche Individualität geht verloren. Bleiben Sie weg vom Computer! Schreiben Sie wieder Liebesbriefe!«

Sie jedenfalls schreibe welche. Das Telefon mag Frau Hayek übrigens auch nicht besonders, aber da könne sie wenigsten noch eine Stimme hören.

(SZ 07.01.2005, 10).

Presseerklärung der DVD e.V. vom 21.02.2005

Steuererklärung per Internet: Elster-Verfahren nach wie vor unsicher

Die Deutsche Vereinigung für Datenschutz stellt mit großem Bedauern fest, dass die begründete Kritik vieler Fachleute am ELSTER-Verfahren zur elektronischen Übermittlung der Steuererklärung offensichtlich nicht ernst genommen wird.

Seit dem 1.1.2005 sind Unternehmen jeglicher Größenordnung (vom Freiberufler bis zum Großkonzern) verpflichtet, dem Finanzamt Steuererklärungen mithilfe einer Software über eine Internet-Verbindung zu übermitteln. Die bisher mögliche Abgabe auf Papier ist nicht mehr zulässig. Es besteht jedoch eine Kulanzregelung bis zum 31.3.2005.

Obwohl »Sicherheit im Internet« heutzutage sogar immer mehr auch dem Laien als wichtiges Thema erscheint, haben sich die Fachleute des Projekts ELSTER anscheinend nur sehr wenig sachkundig mit dem Thema Sicherheit befasst. Bei einer Steueranmeldung wird nicht geprüft, wer diese Daten übermittelt. Jeder X-beliebige kann in schädigender Absicht gefälschte Steuerdaten eines Unternehmens übertragen, sobald er dessen auf jeder Rechnung befindliche Steuernummer kennt. Dass die Datenübertragung immerhin verschlüsselt geschieht, hilft in der Sache dann auch nicht weiter.

Da die Finanzverwaltung anscheinend nicht in der Lage ist, vor Sommer 2006 eine sichere Gesamtlösung zur Verfügung zu stellen, bestünde die einfachste Lösung in der generellen Anerkennung von Steuererklärungen in der bisherigen Papierform. Vom Bundesbeauftragten für den Datenschutz ist jedoch zu erfahren, dass die Länderfinanzverwaltungen dem nicht weisungsberechtigten Bundesministerium der Finanzen diesbezüglich eine Absage erteilt haben. Bestenfalls sollen bei Anträgen betroffener Unternehmen auf Weiterführung per Papier unbillige Härten dadurch vermieden werden, dass das pflichtgemäße Ermessen der Beamten großzügig zu Gunsten der Betroffenen ausgelegt werden soll.

Damit wäre das Recht der Betroffenen auf Sicherheit ins Ermessen der jeweiligen Beamten gestellt, was aus Sicht der DVD ein von Willkür bedrohtes Verfahren darstellt.

Da weder auf die begründete Kritik des Bundesbeauftragten für den Datenschutz noch von Branchenverbänden wie dem Bund der Steuerzahler und BITKOM durch schnelle Umsetzung einer Kontrolle der Zurechenbarkeit reagiert wurde, empfiehlt die Deutsche Vereinigung für Datenschutz daher allen Betroffenen, einen Antrag auf Fortführung der papiergestützten Erklärungen zu stellen.

Die DVD stellt hierfür ein Musterschreiben zur Verfügung. Außerdem sollten Einzugsermächtigungen gegenüber den Finanzämtern widerrufen werden.

Nachfragen zu dieser PE bitte an Karin Schuler, karin@schuler-ds.de.

Musterbrief

An das
Finanzamt [Stadt]
[Straße]
[PLZ Ort]

Antrag auf Abgabe der Umsatzsteuervoranmeldungen in Papierform,
[Steuernummer/n-Liste]

Sehr geehrte Damen und Herren,

hiermit beantrage ich, die monatlichen Umsatzsteuervoranmeldungen weiterhin in Papierform abgeben zu können.

Begründung:
An IT-Verfahren, die sensible Unternehmensdaten und personenbezogene Daten über das Internet verschicken, sind heute hohe Sicherheitsanforderungen zu stellen. Der Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Zurechenbarkeit kommt daher gerade bei Steuerdaten besonders hohe Bedeutung zu. Dabei ist auch zu prüfen, welche Maßnahmen welchen Gefährdungen der Sicherheit entgegenwirken können. So wird im ELSTER-Verfahren nicht die Urheberschaft der Steuererklärung geprüft, so dass ein unberechtigter Dritter allein durch Kenntnis meiner Steuernummer eine gefälschte Steuererklärung für mich abgeben kann.

Auf dieses erhebliche Sicherheitsloch wurde bereits von verschiedenen Seiten hingewiesen. Auch der Bundesbeauftragte für den Datenschutz hat die sofortige Nachbesserung des Verfahrens verlangt, ohne dass das Verfahren bisher um eine sichere Zurechenbarkeitskontrolle ergänzt worden wäre.

Die Forderung, meine Steuererklärungen durch ein unsicheres elektronisches Verfahren vorzunehmen, halte ich daher für eine unbillige Härte.

Vorsorglich widerrufe ich alle bestehenden Einzugsermächtigungen für die o.g. Steuernummern und meine Konten [Aufzählung Kto-Nr. BLZ].

Mit freundlichen Grüßen



Ich will die

Datenschutz Nachrichten

abonnieren!

4 x im Jahr mindestens 36 Seiten

Informationen, Nachrichten, Diskussionen, Meinungen, Buchbesprechungen, Gesetzgebung, Rechtsprechung und einiges mehr

aus der Welt des Datenschutzes

kritisch und bürgerrechtsorientiert.

✂ -

Absender

Name, Zuname: ....

Straße: ....

PLZ, Ort: ....

(Die Angaben werden ausschließlich zur Abwicklung des Abonnements elektronisch verarbeitet. Eine Weitergabe der Daten findet außer gegenüber der Bank bei Bankeinzug nicht statt.)

Deutsche Vereinigung für Datenschutz
Bonner Talweg 33-35

53113 Bonn

Hiermit bestelle ich
ein Jahresabonnement der Zeitschrift
Datenschutz Nachrichten
zum Preis von 32 €/Jahr.

Wenn das Abonnement nicht spätestens drei Monate vor Ende des Kalenderjahres gekündigt wird, verlängert es sich um jeweils ein weiteres Jahr.

Datum: Unterschrift:

Ich zahle durch Bankeinzug vom

Konto bei .... (Bank)

BLZ: .... Konto: ....

Datum: Unterschrift:

Ich weiß, dass ich diese Vereinbarung innerhalb von zehn Tagen schriftlich bei der DVD, Bonner Talweg 33-35, 53113 Bonn, widerrufen kann. Zur Wahrung der Frist genügt die rechtzeitige Absendung.

Datum: Unterschrift: